116TH CONGRESS
1st Session

SENATE

REPORT
116-XX

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION

VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE

WITH ADDITIONAL VIEWS

CONTENTS

Russian Efforts Against Election Infrastructure

I. (U) INTRODUCTION

(U) From 2017 to 2019, the Committee held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access election infrastructure. The Committee sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future. The Committee received testimony from state election officials, Obama administration officials, and those in the Intelligence Community and elsewhere in the U.S. Government responsible for evaluating threats to elections.

II. (U) FINDINGS

1. [redacted] The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure[1] at the state and local level. [redacted] The Committee has seen no evidence that any votes were changed or that any voting machines were manipulated.[2]

2. [redacted]

---

[1] **(U)** The Department of Homeland Security (DHS) defines *election infrastructure* as "storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments, " according to the January 6, 2017 statement issued by Secretary of Homeland Security Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, available at https://www.dhs.gov/news/2017/10/06/statement-secretary-johnson-designation-election-infrastructure-critical. Similarly, the Help America Vote Act (HAVA), Pub. L. No. 107-252, Section 301(b)(1) refers to a functionally similar set of equipment as "voting systems," although the definition excludes physical polling places themselves, among other differences, 52 U.S.C. §21081(b). This report uses the term *election infrastructure* broadly, to refer to the equipment, processes, and systems related to voting, tabulating, reporting, and registration.

[2] [redacted] The Committee has reviewed the intelligence reporting underlying the Department of Homeland Security (DHS) assessment from early 2017 [redacted] The Committee finds it credible.

[3] **(U)** The names of the states the Committee spoke to have been replaced with numbers. DHS and some states asked the Committee to protect state names before providing the Committee with information. The Committee's goal was to get the most information possible, so state names are anonymized throughout this report. Where the report refers to public testimony by Illinois state election officials, that state is identified.

3. **(U)** While the Committee does not know with confidence what Moscow's intentions were, Russia may have been probing vulnerabilities in voting systems to exploit later. Alternatively, Moscow may have sought to undermine confidence in the 2016 U.S. elections simply through the discovery of their activity.

4. **(U)** Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states. The U.S. intelligence apparatus is, by design, foreign-facing, with limited domestic cybersecurity authorities except where the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) can work with state and local partners. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor.

5. **(U)** DHS and FBI alerted states to the threat of cyber attacks in the late summer and fall of 2016, but the warnings did not provide enough information or go to the right people. Alerts were actionable, in that they provided malicious Internet Protocol (IP) addresses to information technology (IT) professionals, but they provided no clear reason for states to take this threat more seriously than any other alert received.

6. **(U)** In 2016, officials at all levels of government debated whether publicly acknowledging this foreign activity was the right course. Some were deeply concerned that public warnings might promote the very impression they were trying to dispel—that the voting systems were insecure.

7. **(U)** Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure. In 2016, cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been. Aging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary. Despite the focus on this issue since 2016, some of these vulnerabilities remain.

8. **(U)** In the face of this threat and these security gaps, DHS has redoubled its efforts to build trust with states and deploy resources to assist in securing elections. Since 2016, DHS has made great strides in learning how election procedures vary across states and how federal entities can be of most help to states. The U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and other groups have helped DHS in this effort. DHS's work to bolster states' cybersecurity has likely been effective, in particular for those states that have leveraged DHS's cybersecurity assessments for election infrastructure, but much more needs to be done to coordinate state, local, and federal knowledge and efforts in order to harden states' electoral infrastructure against foreign meddling.

9. **(U)** To assist in addressing these vulnerabilities, Congress in 2018 appropriated $380 million in grant money for the states to bolster cybersecurity and replace vulnerable

voting machines.[4] When those funds are spent, Congress should evaluate the results and consider an additional appropriation to address remaining insecure voting machines and systems.

10. **(U)** DHS and other federal government entities remain respectful of the limits of federal involvement in state election systems. States should be firmly in the lead for running elections. The country's decentralized election system can be a strength from a cybersecurity perspective, but each operator should be keenly aware of the limitations of their cybersecurity capabilities and know how to quickly and properly obtain assistance.

III. (U) THE ARC OF RUSSIAN ACTIVITIES

[redacted] In its review of the 2016 elections, the Committee found no evidence that vote tallies were altered or that voter registry files were deleted or modified, though the Committee and IC's insight into this is limited. Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. elections [redacted] Throughout 2016 and for several years before, Russian intelligence services and government personnel conducted a number of intelligence-related activities targeting the voting process. [redacted] the Committee found ample evidence to suggest that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in U.S. democratic institutions and voting processes.[5]

[redacted]

- [redacted]

---

[4] **(U)** Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348, 561-562.

[5] **(U)** The Committee has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases. These activities are routinely carried out in the context of private sector breaches.

[6] [redacted] FBI LHM, [redacted]

[7] [redacted] FBI LHM, [redacted]

[8] [redacted] DHS Homeland Intelligence Brief, [redacted]

[9] [redacted] FBI LHM, [redacted]

- [redacted]
- [redacted]

[redacted] Evidence of scanning of state election systems first appeared in the summer prior to the 2016 election. In mid-July 2016, Illinois discovered anomalous network activity, specifically a large increase in outbound data, on a Illinois Board of Elections' voter registry website.[12] Working with Illinois, the FBI commenced an investigation.[13] [redacted] The attack resulted in data exfiltration from the voter registration database.[16]

(U) On August 18, 2016, FBI issued an unclassified FLASH[17] to state technical-level experts on a set of [redacted] suspect IP addresses identified from the attack on Illinois's voter registration databases.[18] [redacted] The FLASH product did not attribute the attack to Russia or any other particular actor.[21]

---

[10] **(U/[redacted])** FBI Electronic Communication, [redacted]

[11] [redacted] FBI LHM, [redacted]

[12] **(U)** DHS briefing for SSCI staff, March 5, 2018.

[13] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 113.

[14] **(U[redacted])** According to the United States Computer Emergency Readiness Team (US-CERT), an SQL injection is "an [redacted] technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code."

[15] **(U)** DHS IIR 4 0050006 17, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016

[16] **(U[redacted])** DHS briefing for SSCI staff, March 5, 2018.

[17] **(U)** FBI FLASH alerts are notifications of potential cyber threats sent to local law enforcement and private industry so that administrators are able to guard their systems against the described threat. FLASHs marked TLP: AMBER are considered sharable with members of the recipients own organization and those with direct need to know.

[18] [redacted] Number T-LD1004-TT, TLP-AMBER, [redacted]

[9] **(U)** *Ibid.*

[20] **(U)** *Ibid.*

[21] R[redacted]wned

(U[redacted]) After the issuance of the August FLASH, the Department of Homeland Security (DHS) and the Multi-State-Information Sharing & Analysis Center (MS-ISAC)[22] asked states to review their log files to determine if the IP addresses described in the FLASH had touched their infrastructure. This request for voluntary self-reporting, in conjunction with DHS analysis of NetFlow activity on MS-ISAC internet sensors, identified another 20 states whose networks had made connections to at least one IP address listed on the FLASH.[23] DHS was almost entirely reliant on states to self-report scanning activity.

[redacted] Former Special Assistant to the President and Cybersecurity Coordinator Michael Daniel said, "eventually we get enough of a picture that we become confident over the course of August of 2016 that we're seeing the Russians probe a whole bunch of different state election infrastructure, voter registration databases, and other related infrastructure on a regular basis."[25] Dr. Samuel Liles, Acting Director of the Cyber Analysis Division within DHS's Office of Intelligence and Analysis (I&A), testified to the Committee on June 21, 2017, that "by late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors."[26]

[redacted]

[22] **(U)** The MS-ISAC is a DHS-supported group dedicated to sharing information between state, local, tribal, and territorial (SLTT) government entities. It serves as the central cybersecurity resource for SLTT governments. Entities join to receive cybersecurity advisories and alerts, vulnerability assessments, incident response assistance, and other services.

[23] **(U[redacted])** DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Governments to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.

[24] **(U)** SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 41.

[25] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on August 31, 2017, p. 39.

[26] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 12.

(U) DHS and FBI issued a second FLASH and a Joint Analysis Report in October that flagged [redacted] suspect IP addresses, many unrelated to Russia.[27] DHS briefers told the Committee that they were intentionally over-reporting out of an abundance of caution, given their concern about the seriousness of the threat. DHS representatives told the Committee, "We were very much at that point in a sort of duty-to-warn type of attitude . . . where maybe a specific incident like this, which was unattributed at the time, wouldn't have necessarily risen to that level. But . . . we were seeing concurrent targeting of other election-related and political figures and political institutions . . . [which] led to what would probably be more sharing than we would normally think to do."[28]

[redacted]

[redacted] DHS assessed that the searches, done alphabetically, probably included all 50 states, and consisted of research on "general election-related web pages, voter ID information, election system software, and election service companies."[31]

[redacted]

---

[27] (U[redacted]) FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems,* October 14, 2016.

[28] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 9-10.

[29] [redacted] FBI LHM, [redacted]

[30] [redacted]

[31] [redacted] DHS Homeland Intelligence Brief, *Update:* [redacted]

[32] [redacted] NSA [redacted] DIRNSA, May 5, 2017. This information was not available to the U.S. government until April 2017.

[33] [redacted]

[34] (U) NSA [redacted] DIRNSA, May 5, 2017.

The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials. [37] In objecting to these tactics, then-Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland reminded the Russian Ambassador that Russia had refused invitations to participate in the official OSCE mission that was to observe the U.S. elections.[38]

[35] **(U)** FBI IIR ; FBI IIR
[36] **(U)** *Ibid.*
[37] **(U)** DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 221-222.
[38] Email, sent November 4, 2016; from ; to: , , , . Subject: Kislyak Protest of FBI Tactics.
[39] **(U)** NSA DIRNSA, May 5, 2017.
[40] **(U)** *Ibid.*
[41]
[42]
[43]

(U) The Committee found no evidence of Russian actors attempting to manipulate vote tallies on Election Day, though again the Committee and IC's insight into this is limited.

(U/[redacted]) In the years since the 2016 election, awareness of the threat, activity by DHS, and measures at the state and local level to better secure election infrastructure have all shown considerable improvement. The threat, however, remains imperfectly understood. In a briefing before Senators on August 22, 2018, DNI Daniel Coats, FBI Director Christopher Wray, then-DHS Secretary Kirstjen Nielsen, and then-DHS Undersecretary for the National Protection and Programs Division Christopher Krebs told Senators that there were no known threats to election infrastructure. However, Mr. Krebs also said that top election vulnerabilities remain, including the administration of the voter databases and the tabulation of the data, with the latter being a much more difficult target to attack.[44] Relatedly, several weeks prior to the 2018 mid-term election, DHS assessed that "numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election."[45]

[redacted]

IV. (U) ELEMENTS OF RUSSIAN ACTIVITIES

A. (U) Targeting Activity

[redacted] Scanning of election-related state infrastructure by Moscow was the most widespread activity the IC and DHS elements observed in the run up to the 2016 election.[48]

- [redacted] In an interview with the Committee, Mr. Daniel stated: "What it mostly looked like to us was reconnaissance. . . . I would have characterized it at the time as sort of conducting the reconnaissance to do the network mapping, to do the topology mapping so

---

[44] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[45] **(U/[redacted])** Homeland Security Intelligence Assessment: Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure, October 11, 2018.
[46] **(U)** DTS 2019-1368, NIC 2019-01, Intelligence Community Assessment: A Summary of the Intelligence Community Report on Foreign Interference as Directed by Executive Order 13848, March 29, 2019. p. 2-3.
[47] **(U)** *Ibid.*
[48] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 12.

that you could actually understand the network, establish a presence so you could come back later and actually execute an operation."[49]

- **(U)** Testifying before the Committee, Dr. Liles characterized the activity as "simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home. A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in . . . [however] a small number of the networks were successfully exploited. They made it through the door."[50]

[redacted] DHS and FBI assessments on the number of affected states evolved since 2016. In a joint FBI/DHS intelligence product published in March 2018, and coordinated with the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the Department of State, the National Intelligence Council, the National Security Agency (NSA), and the Department of Treasury, DHS and FBI assessed [redacted] that Russian intelligence services conducted activity [redacted].[51]

- [redacted] DHS arrived at their initial assessment by evaluating whether the tactics, techniques, and procedures (TTPs) observed were consistent with previously observed Russian TTPs, whether the actors used known Russian-affiliated malicious infrastructure, and whether a state or local election system was the target.[53]

- **(U)** The majority of information examined by DHS was provided by the states themselves. The MS-ISAC gathered information from states that noticed the suspect IPs pinging their systems. In addition, FBI was working with some states in local field offices and reporting back FBI's findings.

- **(U)** If some states evaluated their logs incompletely or inaccurately, then DHS might have no indication of whether they were scanned or attacked. As former-Homeland Security Adviser Lisa Monaco told the Committee, "Of course, the law enforcement and the intelligence community is going to be significantly reliant on what the holders and

---

[49] **(U)** SSCI Transcript of the Interview of Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 44.
[50] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[51] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]
[52] **(U)** *See* chart, *infra*, for information on successful breaches.
[53] **(U)** DHS did not count attacks on political parties, political organizations, or NGOs. For example, the compromise of an email affiliated with a partisan State 13 voter registration organization was not included in DHS's count.

owners and operators of the infrastructure sees on its system [sic] and decides to raise their hand."[54]

[redacted] However, both the IC and the Committee in its own review were unable to discern a pattern in the affected states, [redacted]

(U) Mr. Daniel told the Committee that by late August 2016, he had already personally concluded that the Russians had attempted to intrude in all 50 states, based on the extent of the activity and the apparent randomness of the attempts. "My professional judgment was we have to work under the assumption that they've tried to go everywhere, because they're thorough, they're competent, they're good."[55]

[redacted] Intelligence developed later in 2018 bolstered Mr. Daniel's assessment that all 50 states were targeted. [redacted]

- [redacted]

[54] **(U)** SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 38.
[55] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 40.
[56] [redacted] DHS/FBI Homeland Intelligence Bulletin, [redacted]
[57] **(U)** *Ibid.*
[58] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[59] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, pp. 11-12.
[60] **(U)** DHS briefing for SSCI staff, March 5, 2018.

- [redacted]
- [redacted]

[redacted]

(U) However, IP addresses associated with the August 18, 2016 FLASH provided some indications the activity might be attributable to the Russian government, particularly the GRU:

- [redacted]
- [redacted]
- **(U/[redacted])** One of the Netherlands-based [redacted] "exhibited the same behavior from the same node over a period of time. . . . It was behaving like . . . the same user or group of users was using this to direct activity against the same type of targets," according to DHS staff.[69]

---

[61] **(U)** *Ibid.*
[62] **(U)** *Ibid.*
[63] **(U)** *Ibid.*
[64] **(U)** *Ibid.*
[65] [redacted]
[66] [redacted] FBI IIR
[67] **(U)** Cyber Threat Intelligence Integration Center (CTIIC) Cyber Threat Intelligence Summary, October 7, 2016.
[68] **(U)** *Ibid.*
[69] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.

- [redacted]

[redacted] The IC's confidence level about the attribution of the attacks evolved over 2017 and into 2018. [redacted]

- [redacted]

- [redacted]

[redacted] The Committee reached out to the 21 states that DHS first identified as targets of scanning activity to learn about their experiences. Election officials provided the Committee

---

[70] **(U)** DHS Electronic Communication, December 19, 2016, email from: DHS/NCCIC; to: CIA.
[71] [redacted]
[72] [redacted]
[73] [redacted] DHS Intelligence Assessment, *Hostile Russian Cyber Targeting of Election Infrastructure in 2016; Probable Non-State Actors Attempt Disruption*, May 3, 2017.
[74] **(U)** *Ibid.*
[75] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.
[76] [redacted] DHS arrived at their initial assessment of 21 states affected by adding the eleven plus seven states, plus the three where scanning activity appeared directed at less specifically election-focused infrastructure.
[77] **(U)** SSCI conference call with DHS and FBI, March 29, 2018.

details about the activity they saw on their networks, and the Committee compared that accounting to DHS's reporting of events.[78] Where those accounts differed is noted below. The scanning activity took place from approximately June through September 2016.

STATE	OBSERVED ACTIVITY[79]
Illinois	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 2	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 3	**(U)** According to State 3 officials, cyber actors using infrastructure identified in the August FLASH conducted scanning activity.[80] State 3 officials noticed "abnormal behavior" and took action to block the related IP addresses.[81] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[82]
State 4	**(U)** *See infra,* "Two Unexplained Events" for a detailed description.
State 5	**(U)** Cyber actors using infrastructure identified in the August FLASH scanned "an old website and non-relevant archives," according to the State 5 Secretary of State's office.[83] The following day, State 5 took action to block the IP address.[84] [redacted] DHS, however, reported GRU scanning activity on two separate State 5 Secretary of State websites, plus targeting of a District Attorney's office[85] in a particular city.[86] Both the websites appear to be current addresses for the State 5 Secretary of State's office.
State 6	**(U)** According to State 6 officials, cyber actors using infrastructure identified in the August FLASH scanned[87] the entire state IT infrastructure, including by using the Acunetix tool, but the "affected systems" were the Secretary of State's

[78] **(U)** DHS briefed Committee staff three times on the attacks, and staff reviewed hundreds of pages of intelligence assessments.

[79] **(U)** Slight variation between what states and DHS reported to the Committee is an indication of one of the challenges in election cybersecurity. The system owners—in this case, state and local administrators—are in the best position to carry out comprehensive cyber reviews, but they often lack the expertise or resources to do so. The federal government has resources and expertise, but the IC can see only limited information about inbound attacks because of legal restrictions on operations inside the United States.

[80] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.

[81] **(U)** *Ibid.*

[82] **(U)** DHS briefing for Committee staff on March 5, 2018.

[83] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.

[84] **(U)** *Ibid.*

[85] **(U/[redacted])** Briefers suggested the "most wanted" list housed on the District Attorney's website may have in some way been connected to voter registration. The exact nature of this connection, including whether it was a technical network connection or whether databases of individuals with felony convictions held by the District Attorney's office had voting registration implications, is unclear.

[86] **(U)** DHS briefing for Committee staff on March 5, 2018.

[87] **(U)** State 6 officials did not specify, but in light of the DHS assessment, they likely meant SQL injection.

	web application and the election results website.[88] If the penetration had been successful, actors could have manipulated the unofficial display of the election tallies.[89] State officials believed they would have caught any inconsistency quickly.[90] State 6 became aware of this malicious activity and alerted partners.[91] [redacted] DHS reported that GRU actors scanned State 6, then unsuccessfully attempted many SQL injection attacks. State 6 saw the highest number of SQL attempts of any state.
State 7	**(U)** According to State 7 officials, cyber actors using infrastructure identified in the August FLASH scanned public-facing websites, including the "static" election site.[92] It seemed the actors were "cataloging holes to come back later," according to state election officials.[93] State 7 became aware of this malicious activity after receiving an FBI alert.[94] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[95]
State 8	**(U)** According to State 8 officials, cyber actors using infrastructure identified in the August FLASH scanned a State 8 public election website on one day.[96] State 8 officials described the activity as heightened but not particularly out of the ordinary.[97] State 8 became aware of this malicious activity after receiving an alert.[98] [redacted]
State 9	**(U)** According to State 9 officials, cyber actors using infrastructure identified in an October MS-ISAC advisory[101] scanned the statewide voter registration

[88] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[89] **(U)** *Ibid.*
[90] **(U)** *Ibid.*
[91] **(U)** *Ibid.*
[92] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[93] **(U)** *Ibid.*
[94] **(U)** *Ibid.*
[95] **(U)** DHS briefing for Committee staff on March 5, 2018.
[96] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[97] **(U)** *Ibid.*
[98] **(U)** *Ibid.*
[99] **(U)** DHS briefing for Committee staff on March 5, 2018.
[100] **(U)** *Ibid.*
[101] **(U)** While the Committee was unable to review the specific indicators shared with State 9 by the MS-ISAC in October, the Committee believes at least one of the relevant IPs was originally named in the August FLASH because of technical data held by DHS which was briefed to the Committee.

	system.[102] Officials used the analogy of a thief casing a parking lot: they said the car thief "didn't go in, but we don't know why."[103] State 9 became aware of this malicious activity after receiving an alert.[104] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[105]
State 10	**(U)** According to State 10 officials, cyber actors using infrastructure identified in the August FLASH conducted activity that was "very loud," with a three-pronged attack: a Netherlands-based IP address attempted SQL injection on all fields 1,500 times, a U.S.-based IP address attempted SQL injection on several fields, and a Poland-based IP address attempted SQL injection on one field 6-7 times.[106] State 10 received relevant cybersecurity indictors from MS-ISAC in early August, around the same time that the attacks occurred.[107] State 10's IT contractor attributed the attack to Russia and suggested that the activity was reminiscent of other attacks where attackers distract with lots of noise and then "sneak in the back."[108] **(U)** State 10, through its firewall, blocked attempted malicious activity against the online voter registration system and provided logs to the National Cybersecurity and Communications Integration Center (NCCIC)[109] and the U.S. Computer Emergency Readiness Team (US-CERT).[110] State 10 also brought in an outside contractor to assist.[111] [redacted] DHS confirmed GRU SQL injection attempts against State 10's voter services website on August 5 and said that the attack was blocked after one day by State 10's firewall.[112]
State 11	**(U)** According to State 11 officials, they have seen no evidence of scanning or attack attempts related to election infrastructure in 2016.[113] While State 11 officials noted an IP address "probing" state systems, activity which was "broader than state election systems," State 11 election officials did not provide specifics on which systems.[114]

[102] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[103] **(U)** *Ibid.*
[104] **(U)** *Ibid.*
[105] **(U)** DHS briefing for Committee staff on March 5, 2018.
[106] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 10], November 29, 2017.
[107] **(U)** *Ibid.*
[108] **(U)** *Ibid.*
[109] **(U)** NCCIC is DHS's cyber watch center.
[110] **(U)** *Ibid.*
[111] **(U)** *Ibid.*
[112] **(U)** DHS briefing for Committee staff on March 5, 2018.
[113] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[114] **(U)** *Ibid.*

	[redacted] DHS reported GRU scanning activity on the Secretary of State domain.[115]
State 12	**(U)** Cyber actors using infrastructure identified in the August FLASH conducted scanning activity that "lasted less than a second and no security breach occurred," according to State 12 officials.[116] State 12 became aware of this malicious activity after being alerted to it.[117] [redacted] DHS reported that because of a lack of sensor data related to this incident, they relied on NetFlow data, which provided less granular information.[118] DHS's only clear indication of GRU scanning on State 12's Secretary of State website came from State 12 self-reporting information to MS-ISAC after the issuance of the August FLASH notification.[119]
State 13	**(U)** According to State 13 officials, they have seen no evidence of scanning or attack attempts related to state-wide election infrastructure in 2016.[120] [redacted]
State 14	[redacted] MS-ISAC passed DHS reports of communications between a suspect IP address used by the GRU at the time and the State 14 election commission webpage, but no indication of a compromise.[123] In addition, DHS was informed of activity relating to separate IP addresses in the August FLASH,

[115] **(U)** DHS briefing for Committee staff on March 5, 2018.
[116] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[117] **(U)** *Ibid.*
[118] **(U)** DHS briefing for Committee staff on March 5, 2018.
[119] **(U)** *Ibid.*
[120] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[121] **(U)** FBI IIR [redacted] DHS briefing for Committee staff on March 5, 2018.
[122] [redacted]; DHS briefing for Committee staff on March 5, 2018. For more information on decisions by DHS to exclude certain activity in its count of 21 states, *see* text box, *infra*, "DHS Methodology for Identifying States Touched by Russian Cyber Actors."
[123] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]; DHS briefing for Committee staff on March 5, 2018.

	including attempted Domain Name System (DNS) lookups and potentially malicious emails, some dating back to January 2016.[124]
State 15	**(U)** State 15 officials were not aware that the state was among those targeted until they were notified.[125] State 15's current lead election official was not in place during the 2016 election so they had little insight into any scanning or attempted intrusion on their systems. State 15 officials said that generally they viewed 2016 as a success story because the attempted infiltration never got past the state's four layers of security. [redacted] DHS reported broad GRU scanning activity on State 15 government domains.[126]
State 16	**(U)** According to State 16 officials, cyber actors using infrastructure identified in the October FLASH conducted scanning activity against a state government network.[127] [redacted] DHS reported information on GRU scanning activity based on a self-report from State 16 after the issuance of the October FLASH.[128]
State 17	**(U)** State 17 officials reported nothing "irregular, inconsistent, or suspicious" leading up to the election.[129] While State 17 IT staff received an MS-ISAC notification, that notification was not shared within the state government.[130] [redacted] DHS reported GRU scanning activity on an election-related domain.[131]
State 18	**(U)** State 18 election officials said they observed no connection from the IP addresses listed in the election-related notifications.[132] [redacted] DHS reported indications of GRU scanning activity on a State 18 government domain.[133]
State 19	**(U)** According to State 19 officials, cyber actors using infrastructure identified in October by MS-ISAC conducted scanning activity. State 19 claimed this activity was "blocked," but did not elaborate on why or how it was blocked.[134]

[124] **(U/[redacted])** DHS IIR 4 019 0012 17, *Cyber Activity Targeting [State 14] Government Networks from Internet Protocol Addresses Associated with Targeting State Elections Systems*, October 21, 2016.
[125] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 15], March 12, 2018.
[126] **(U)** DHS briefing for Committee staff on March 5, 2018.
[127] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[128] **(U)** DHS briefing for Committee staff on March 5, 2018.
[129] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[130] **(U)** *Ibid.*
[131] **(U)** DHS briefing for Committee staff on March 5, 2018.
[132] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 18], December 8, 2017.
[133] **(U)** DHS briefing for Committee staff on March 5, 2018.
[134] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 19], December 1, 2017.

	[redacted] DHS reported indications of GRU scanning activity on two separate State 19 government domains.[135]
State 20	**(U)** According to State 20 officials, cyber actors using infrastructure identified in October by MS-ISAC were "knocking" on the state's network, but no successful intrusion occurred.[136] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[137]
State 21	**(U)** State 21 officials received indicators from MS-ISAC in October 2016. They said they were not aware the state was among those targeted until notified.[138] [redacted] DHS reported GRU scanning activity on an election-related domain as well as at least one other government system connected to the voter registration system.[139]

[redacted] Neither DHS nor the Committee can ascertain a pattern to the states targeted, lending credence to DHS's later assessment that all 50 states probably were scanned. DHS representatives told the Committee that "there wasn't a clear red state-blue state-purple state, more electoral votes, less electoral votes" pattern to the attacks. DHS acknowledged that the U.S. Government does not have perfect insight, and it is possible the IC missed some activity or that states did not notice intrusion attempts or report them.[140] [redacted]

[redacted]

---

[135] **(U)** DHS briefing for Committee staff on March 5, 2018.
[136] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[137] **(U)** DHS briefing for Committee staff on March 5, 2018.
[138] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.
[139] **(U)** DHS briefing for Committee staff on March 5, 2018.
[140] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 25.
[141] [redacted]
[142] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 21.

(U/[redacted]) As of October 2018, the IC and DHS were looking for evidence of threats to election systems, [redacted]. An October 11, 2018 DHS Intelligence Assessment reported the following:

> *We judge that numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election. We are aware of a growing volume of malicious activity targeting election infrastructure in 2018, although we do not have a complete baseline of prior years to determine relative scale of the activity. Much of our understanding of cyber threats to election infrastructure is due to proactive sharing by state and local election officials, as well as more robust intelligence and information sharing relationships amongst the election community and within the Department. The observed activity has leveraged common tactics—the types of tactics that are available to nation-state and non-state cyber actors, alike—with limited success in compromising networks and accounts. We have not attributed the activity to any foreign adversaries, and we continue to work to identify the actors behind these operations. At this time, all these activities were either prevented or have been mitigated.*

(U/[redacted]) Specifically:

> *Unidentified cyber actors since at least April 2018 and as recently as early October continue to engage in a range of potential elections-related cyber incidents targeting election infrastructure using spear-phishing, database exploitation techniques, and denial of service attacks, possibly indicating continued interest in compromising the availability, confidentiality, and integrity of these systems. For example, on 24 August 2018, cybersecurity officials detected multiple attempts to illegally access the State of Vermont's Online Voter Registration Application (OLVR), which serves as the state's resident voter registration database, according to DHS reporting. The malicious activity included one Cross Site Scripting attempt, seven Structured Query Language (SQL) injection attempts, and one attempted Denial of Service (DoS) attack. All attempts were unsuccessful.*[143]

(U/[redacted]) In summarizing the ongoing threat to U.S. election systems, DHS further said in the same product, "We continue to assess multiple elements of U.S. election infrastructure are potentially vulnerable to cyber intrusions."[144]

B. (U) Russian Access to Election Infrastructure

---

[143] (U/[redacted]) DHS, Homeland Security Intelligence Assessment, *Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure*, October 11, 2018.
[144] (U) *Ibid.*

(U) The January 6, 2017 Intelligence Community Assessment (ICA), "Assessing Russian Activities and Intentions in Recent U.S. Elections," states:

> *Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.*[145]

[redacted] Based on the Committee's review of the ICA, the Committee concurs with this assessment. The Committee found that Russian-affiliated cyber actors gained access to election infrastructure systems across two states, including successful extraction of voter data. However, none of these systems were involved in vote tallying.

1. (U) Russian Access to Election Infrastructure: Illinois

(U) In June 2016, Illinois experienced the first known breach by Russian actors of state election infrastructure during the 2016 election.[146] As of the end of 2018, the Russian cyber actors had successfully penetrated Illinois's voter registration database, viewed multiple database tables, and accessed up to 200,000 voter registration records.[147] The compromise resulted in the exfiltration of an unknown quantity of voter registration data.[148] Russian cyber actors were in a position to delete or change voter data, but the Committee is not aware of any evidence that they did so.[149]

- [redacted] DHS assesses with high confidence that the penetration was carried out by Russian actors.[150]
- **(U/[redacted])** The compromised voter registration database held records relating to 14 million registered voters, [redacted]. The records exfiltrated included information on each voter's name, address, partial social security number, date of birth, and either a driver's license number or state identification number.[151]

---

[145] **(U)** Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. iii.
[146] **(U/[redacted])** DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.
[147] **(U)** "Illinois election officials say hack yielded information on 200,000 voters," [Local Newspaper], August 29, 2016.
[148] **(U)** DHS IIR [redacted] SCI Open Hearing on June 21, 2017, p 110
[149] **(U)** State Board of Elections, *Illinois Voter Registration System Records Breached*, August 31, 2016. As reflected elsewhere in this report, the Committee did not undertake its own forensic analysis of the Illinois server logs to corroborate this statement; SSCI interview with DHS and CTIIC, February 27, 2018, p. 24.
[150] **(U)** *See infra*, "Russian Scanning and Attempted Access to Election-Related Infrastructure" for a complete discussion on attribution related to the set of cyber activity linked to the infrastructure used in the Illinois breach.
[151] **(U/[redacted])** FBI IIR [redacted] DHS Intelligence Assessment, May 3, 2017, 0144-17, p. 2.

- [redacted] DHS staff further recounted to the Committee that "Russia would have had the ability to potentially manipulate some of that data, but we didn't see that." [152] Further, DHS staff noted that "the level of access that they gained, they almost certainly could have done more. Why they didn't . . . is sort of an open-ended question. I think it fits under the larger umbrella of undermining confidence in the election by tipping their hand that they had this level of access or showing that they were capable of getting it."[153]

- **(U)** According to a Cyber Threat Intelligence Integration Center (CTIIC) product, Illinois officials "disclosed that the database has been targeted frequently by hackers, but this was the first instance known to state officials of success in accessing it."[154]

(U) In June 2017, the Executive Director of the Illinois State Board of Elections (SBE), Steve Sandvoss, testified before the Committee about Illinois's experience in the 2016 elections.[155] He laid out the following timeline:

- **(U)** On June 23, 2016, a foreign actor successfully penetrated Illinois's databases through an SQL attack on the online voter registration website. "Because of the initial low-volume nature of the attack, the State Board of Election staff did not become aware of it at first."[156]

- **(U)** Three weeks later, on July 12, 2016, the IT staff discovered spikes in data flow across the voter registration database server. "Analysis of the server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of our paperless online voter application website."[157]

- **(U)** On July 13, 2016, IT staff took the website and database offline, but continued to see activity from the malicious IP address.[158]

- **(U)** "Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th [2016], when they abruptly ceased."[159]

---

[152] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 14.
[153] **(U)** *Ibid.*
[154] **(U)** CTIIC Cyber Threat Intelligence Summary, August 18, 2016.
[155] **(U)** SSCI Open Hearing on June 21, 2017. The Committee notes that, in his testimony, Mr. Sandvoss said Illinois still had not been definitively told that Russia perpetrated the attack, despite DHS's high confidence. The Committee also notes that DHS eventually provided a briefing to states during which DHS provided further information on this topic, including the DHS high-confidence attribution to Russia.
[156] **(U)** *Ibid.*, p. 110.
[157] **(U)** *Ibid.*
[158] **(U)** *Ibid.*, p. 111.
[159] **(U)** *Ibid.*

- **(U)** On July 19, 2016, the election staff notified the Illinois General Assembly and the Attorney General's office.

- **(U)** Approximately a week later, the FBI contacted Illinois.[160]

- **(U)** On July 28, 2016, both the registration system and the online voter registration became fully functional again.[161]

2. (U) Russian Access to Election Infrastructure: State 2

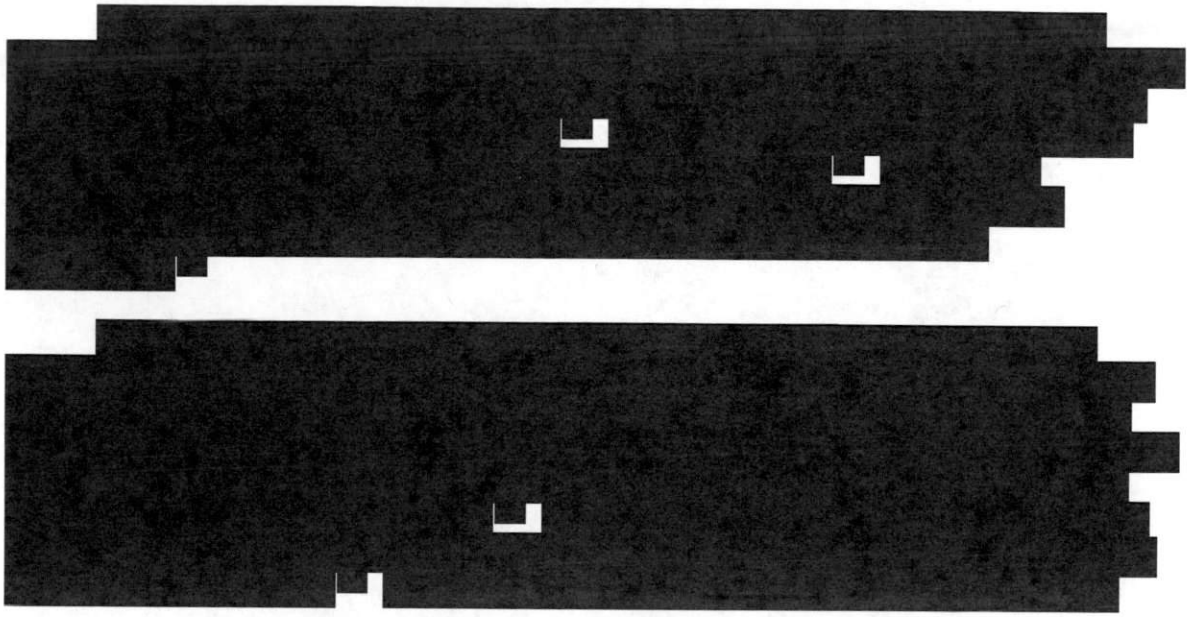
[redacted]

[redacted] Separately, GRU cyber actors breached election infrastructure in State 2. [redacted]

- [redacted]

---

[160] **(U)** *Ibid.*, p. 113.
[161] **(U)** *Ibid.*, p. 112.
[162] **(U/** [redacted] **)** FBI Electronic Communication, [redacted]
[163] **(U)** *Ibid.*
[164] [redacted]
[165] **(U)** FBI Briefing on [State 2] Election Systems, June 25, 2018.
[166] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[167] **(U)** *Ibid.*
[168] **(U)** *Ibid.*
[169] **(U)** *Ibid.*
[170] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 16.
[171] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, compartmented session.



(U) FBI and DHS Interactions with State 2[179]	
August 18, 2016	**(U)** FBI FLASH notification identified IP addresses targeting election offices.[180]
August 24, 2016	**(U)** State 2 Department of State received the FLASH from National Association of Secretaries of State.[181]
August 26, 2016	**(U)** State 2 Department of State forwarded FLASH to counties and advised them to block the IP addresses.[182] Separately, determined one of the listed IP addresses scanned its system.[183] subsequently discovered suspected intrusion activity and contacted the FBI.[184]

[172] **(U)** *Ibid.*
[173] **(U)** *Ibid.*
[174] **(U)** *Ibid.*
[175] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[176] **(U)** *Ibid.*
[177] *Ibid. See also* EB-0004893-LED
[178] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 42.
[179] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[180] **(U)** FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER,
[181] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 4.
[182] **(U)** *Ibid.*, pp. 4-5.
[183] **(U)** *Ibid.*, p. 5.
[184] **(U)** *Ibid.*

August 31, 2016	[redacted] FBI opened its investigation on the [redacted] and "conducted outreach to State 2 county election officials to discuss individual security postures and any suspicious activity."[185] FBI outreach reveals that one State 2 county—County A—was scanned.[186]
September 30, 2016	[redacted] FBI held a conference call with county election officials to advise of the attempt to probe County A.[187] FBI also notified state and local officials of available DHS services.[188]
October 4, 2016	[redacted] County B's IT administrator contacted FBI regarding a potential intrusion.[189] According to the FBI, "Of particular concern, the activity included a connection to a county voting, testing, and maintenance server used for poll worker classes."[190]
October 14, 2016	**(U)** FBI shared County B indicators by issuing a FLASH.[191]
December 29, 2016	**(U)** DHS and FBI released a Joint Analysis Report (JAR) on the "GRIZZLY STEPPE" intrusion set; report represents the first IC attribution of state election-related systems to the Russians.[192]
[redacted]	[redacted]
June 2017	**(U)** DHS notified State 2 counties of a possible intrusion "as part of a broader notification to 122 entities identified as spearphishing victims in an intelligence report."[194]

[185] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 5.
[186] **(U)** *Ibid.*
[187] **(U)** *Ibid.*, pp. 5-6.
[188] **(U)** *Ibid.*, p. 6.
[189] **(U)** *Ibid.*
[190] **(U)** *Ibid.*
[191] **(U//** [redacted] **)** FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]
[192] **(U)** DHS/FBI, Joint Analysis Report, JAR-16-20296A, GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016.
[193] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[194] **(U)** *Ibid.*

July 2017	**(U)** FBI published a FLASH report warning of possible spearphishing.[195]
November 2017	**(U)** FBI and DHS participated in the first meeting of the State 2 elections task force.[196]
February 2018	**(U)** FBI requested direct engagement with Counties B, C, and D, including a reminder of available DHS services.[197]
March 2018	**(U)** FBI reports that "our office engaged" the affected counties through the local FBI field office.[198] The FBI could not provide any further detail on the substance of these engagements to the Committee.
May 29, 2018	[redacted] FBI provided a SECRET Letterhead Memo to DHS "formally advising of our investigation into the intrusion [redacted], the reported intrusion at County B, and suspected compromises of Counties C and D."[199]
June 11, 2018	**(U)** FBI reports that as of June 11, 2018, Counties A, B, C, and D had not accepted DHS services.[200]

[redacted]

[redacted]

[195] **(U)** FBI FLASH, Alert Number EB-000083-LD, TLP-AMBER, [redacted]. *See* DTS 2018-3174.
[196] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[197] **(U)** *Ibid.*, p. 6.
[198] **(U)** *Ibid.*, p. 34.
[199] **(U)** *Ibid.*, pp. 8-9.
[200] **(U)** *Ibid.*, p. 20.
[201] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 20-21.
[202] [redacted] DHS briefing for SSCI staff, March 5, 2018.

- **(U)** State 2's Secretary of State and Election Director told the Committee in December 2017 that there was "never an attack on our systems." "We did not see any unusual activities. I would have known about it personally."[203] State 2 did not want to share with the Committee its cybersecurity posture, but state officials communicated that they are highly confident in the security of their systems.[204]

- **(U)** State 2's election apparatus is highly decentralized, with each county making its own decisions about acquiring, configuring, and operating election systems.[205]

- **(U)** As of August 9, 2018, DHS was complimentary of the steps State 2 had taken to secure its voting systems, including putting nearly all counties on the ALBERT sensor system, joining the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and using congressionally appropriated funds plus additional state funds to hire cybersecurity advisors.[206]

C. (U) Russian Efforts to Research U.S. Voting Systems, Processes, and Other Elements of Voting Infrastructure

[redacted]

- [redacted]

---

[203] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 2], December 1, 2017.
[204] **(U)** *Ibid.*
[205] **(U)** *Ibid.*
[206] **(U)** DTS 2018-2581, Memorandum for the Record, Telephone call with DHS, August 9, 2018.
[207] [redacted] FBI LHM, [redacted]
[208] **(U)** *Ibid.*, p. 5.
[209] [redacted] Note: "FISA" refers to electronic surveillance collected on a foreign power or an agent of a foreign power pursuant to the Foreign Intelligence Surveillance Act of 1978. This collection could have come from landlines, electronic mail accounts, or mobile phones used by personnel at a foreign embassy (i.e., an "establishment" FISA) or used by personnel associated with a foreign power (i.e., "agents of a foreign power"). This FISA collection would have been approved by the Foreign Intelligence Surveillance Court ("FISC"), effectuated by FBI, and then could also have been shared with NSA or CIA, or both, depending on the foreign target.

-
-
- It is unknown if Tarantsov attended the events.
-
-

D. (U) Russian Activity Directed at Voting Machine Companies

---

[210] FBI LHM,
[211] FBI LHM,
[212] **(U)** *Ibid.*
[213] **(U)** *Ibid.*, p. 3.
[214] **(U)** *Ibid.*, p. 4.
[215] **(U)** *Ibid.*
[216] **(U)** *Ibid.*, p. 5.
[217]

[redacted] Russian government actors engaged in [redacted] attacks on election systems, [redacted].

- [redacted] FBI reported that "between December 2015 and June 2016, [redacted] DHS further told the Committee that malicious cyber actors had scanned [redacted] a widely-used vendor of election systems.[219]

- [redacted]

E. (U) Russian Efforts to Observe Polling Places

[redacted] Department of State were aware that Russia was attempting to send election observers to polling places in 2016. The true intention of these efforts is unknown.

- [redacted]

---

218 [redacted] FBI Electronic Communication, [redacted]

219 **(U)** DHS briefing for SSCI staff, March 5, 2018.

220 [redacted]

221 **(U)** *Ibid.*

222 **(U)** *Ibid.*

223 **(U)** NSA [redacted] DIRNSA, May 5, 2017, p. 3.

224 **(U)** *Ibid.*, pp. 1-3.

225 **(U)** FBI IIR [redacted]

226 **(U)** *Ibid.*

- [redacted] The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials.[227] For example, in September 2016, the State 5 Secretary of State denied a request by the Russian Consul General to allow a Russian government official inside a polling station on Election Day to study the U.S. election process, according to State 5 officials.[228] [redacted]

[redacted] n mission.[231]

[redacted] nterfere

- [redacted]

---

[227] **(U)** DTS 2018-2152, SSCI Transcript of the Interview of Andrew McCabe, Former Deputy Director of the Federal Bureau of Investigation, February 14, 2018, pp. 221-222.
[228] **(U)** *Ibid.*
[229] **(U)** *Ibid.*
[230] **(U)** *Ibid.*
[231] [redacted] Email, sent November 4, 2016; from [redacted]; to: [redacted]; subject: Kislyak Protest of FBI Tactics.
[232] [redacted] Email, sent: September 13, 2016; from: [redacted] subject: Russia visas/travel.
[233] **(U)** *Ibid.*
[234] **(U)** *Ibid.*
[235] [redacted] Email Sent: Monday, November 7, 2016, 8:11 AM; from: [redacted]; to: [redacted] subject: RE: Kislyak Protest of FBI Tactics --- SECRET//NOFORN.

F.

G. (U) Russian Activity Possibly Related to a Misinformation Campaign on Voter

---

[236] DTS 2018-3952; MFR of Interview with Randy Coleman, December 5, 2018.
[237] **(U)** NSA DIRNSA, May 5, 2017.
[238] **(U)** *Ibid.*
[239] **(U)** SSCI Interview with DHS and CTIIC, February 27, 2018, pp. 47-48.
[240] FBI IIR
[241] **(U//**) FBI LHM,
[242] **(U)** *Ibid.*

[redacted]

(U) The declassified, January 6, 2017, Intelligence Community Assessment also highlighted preparations related to voter fraud, noting that Russian diplomats "were prepared to publicly call into question the validity of the results" and that "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity."[245]

(U) During a 2017 election, State 17 saw bot activity on social media, including allegations of voter fraud, in particular on Reddit. State 17 had to try to prove later that there was no fraud.[246]

H. (U) Two Unexplained Events

1. (U) Cyber Activity in State 22

[redacted]

---

[243] [redacted]

[244] [redacted]

[245] **(U)** Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. 2.

[246] **(U)** *See* Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018. The Committee notes it is conducting a related investigation into the use of social media by Russian-government affiliated entities.

[247] **(U)** The Fusion Center model is a partnership between DHS and state, local, tribal, and territorial entities. They serve as a focal point for "the receipt, analysis, gathering, and sharing of threat-related information."

[248] **(U)** CTIIC Cyber Threat Intelligence Summary/Cyber Threats in Focus, Malicious Cyber Activity on Election-Related Computer Networks Last Spring Possibly Linked to Russia, October 7, 2016; DHS, IIR 4 019 0147 16, September 28, 2016.

[249] **(U)** *Ibid.*

[250] **(U)** *Ibid.*

2. (U) Cyber Activity in State 4

(U[redacted]) State 4 officials, DHS, and FBI in the spring and summer of 2016, struggled to understand who was responsible for two rounds of cyber activity related to election infrastructure. Eventually, one set of cyber activity was attributed to Russia and one was not.

(U[redacted]) First, in April of 2016, a cyber actor successfully targeted State 4 with a phishing scam. After a county employee opened an infected email attachment, the cyber actor stole credentials, which were later posted online.[251] Those stolen credentials were used in June 2016 to penetrate State 4's voter registration database.[252] A CTIIC product reported the incident as follows: "An unknown actor viewed a statewide voter registration database after obtaining a state employee's credentials through phishing and keystroke logging malware, according to a private-sector DHS partner claiming secondhand access. The actor used the credentials to access the database and was in a position to modify county, but not statewide, data."[253]

(U[redacted]) DHS analysis of forensic data provided by a private sector partner discovered malware on the system, and State 4 shut down the voter registration system for about eight days to contain the attack.[254] State 4 officials later told the Committee that that while the cyber actor was able to successfully log in to a workstation connected to election related infrastructure, additional credentials would have been needed for the cyber actor to access the voter registration database on that system.[255]

(U) At first, FBI told State 4 officials that the attack may have originated from Russia, but the ties to the Russian government were unclear. "The Bureau described the threat as 'credible' and significant, a spokesman for State 4 Secretary of State said."[256] State 4 officials also told press that the hacker had used a server in Russia, but that the FBI could not confirm the

---

[251] **(U)** [redacted].

[252] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 38.

[253] [redacted] Cyber Threat Intelligence Integration Center (CTIIC), Compromised State Election Networks, November 2, 2016, p. 1.

[254] **(U[redacted])** DHS IIR 4 005 0829 16, *A [redacted] U.S. State Government's Election System Targeted by Malicious Activity*, September 9, 2016; Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[255] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[256] **(U)** [redacted]

attack was tied to the Russian government.[257] DHS and FBI later assessed it to be criminal activity, with no definitive tie to the Russian government.[258]

[redacted] Subsequently, Russian actors engaged in the same scanning activity as seen in other states, but directed at a domain affiliated with a public library.[259] Officials saw no effective penetration of the system. DHS has low confidence that this cyber activity is attributable to the Russian intelligence services because the target was unusual and not directly involved in elections.[260] [redacted]

V. (U) RUSSIAN INTENTIONS

(U) Russian intentions regarding U.S. election infrastructure remain unclear. Russia might have intended to exploit vulnerabilities in election infrastructure during the 2016 elections and, for unknown reasons, decided not to execute those options. Alternatively, Russia might have sought to gather information in the conduct of traditional espionage activities. Lastly, Russia might have used its activity in 2016 to catalog options or clandestine actions, holding them for use at a later date. Based on what the IC knows about Russia's operating procedures and intentions more broadly, the IC assesses that Russia's activities against U.S. election infrastructure likely sought to further their overarching goal: undermining the integrity of elections and American confidence in democracy.

- **(U)** Former-Homeland Security Adviser Lisa Monaco told the Committee that "[t]here was agreement [in the IC] that one of the motives that Russia was trying to do with this active measures campaign was to sow distrust and discord and lack of confidence in the voting process and the democratic process."[262]

- [redacted] DHS representatives told the Committee that "[w]e see . . . Russians in particular obviously, gain access, learn about the environment, learn about what systems are interconnected, probing, the type of intelligence preparation of the environment that you would expect from an actor like the Russians. So certainly the context going forward

---

[redacted]

[258] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 40.

[259] (U) [redacted]

[260] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]

[261] (U) *Ibid.*

[262] (U) SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 30.

is a concern of what they might have learned and how much more they know about the systems."[263]

- [redacted] Mr. McCabe told the Committee that it seemed to him like "classic Russian cyber espionage. . . . [They will] scrape up all the information and the experience they possibly can," and "they might not be effective the first time or the fifth time, but they are going to keep at it until they can come back and do it in an effective way."[264]

- [redacted] Mr. Daniel told the Committee:

> *While any one voting machine is fairly vulnerable, as has been demonstrated over and over again publicly, the ability to actually do an operation to change the outcome of an election on the scale you would need to, and do it surreptitiously, is incredibly difficult. A much more achievable goal would be to undermine confidence in the results of the electoral process, and that could be done much more effectively and easily. . . . A logical thing would be, if your goal is to undermine confidence in the U.S. electoral system—which the Russians have a long goal of wanting to put themselves on the same moral plane as the United States . . . one way would be to cause chaos on election day. How could you start to do that? Mess with the voter registration databases.*[265]

- [redacted] Ms. Monaco further echoed that concern:

> *Well, one of the things I was worried about—and I wasn't alone in this—is kind of worst-case scenarios, which would be things like the voter registration databases. So if you're a state and local entity and your voter registration database is housed in the secretary of state's office and it is not encrypted and it's not backed up, and it says Lisa Monaco lives at Smith Street and I show up at my [polling place] and they say 'Well we don't have Ms. Monaco at Smith Street, we have her at Green Street,' now there's difficulty in my voting. And if that were to happen on a large scale, I was worried about confusion at polling places, lack of confidence in the voting system, anger at a large scale in some areas, confusion, distrust. So there was a whole sliding scale of*

---

[263] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 15.
[264] **(U)** DTS 2018-2152, SSCI Transcript of the Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 224-225.
[265] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, pp. 27, 34.

horribles just when you're talking about voter registration databases.[266]

- [redacted]

(U) Chaos on Election Day: Three Scenarios

[redacted] Mr. Daniel said that in the early fall of 2016, a policy working group was looking at three scenarios:

> *One was, could the Russians do something to the voter registration databases that could cause problems on Election Day? An example of that would be, could you go in and flip the digits in everybody's address, so that when they show up with their photo ID it doesn't match what's in the poll book? It doesn't actually prevent people from voting. In most cases you'll still get a provisional ballot, but if this is happening in a whole bunch of precincts for just about everybody showing up, it gives the impression that there's chaos.*[268]
>
> *A second one was to do a variant of the penetrating voting machines, except this time what you do is you do a nice video of somebody conducting a hack on a voting machine and showing how you could do that hack and showing them changing a voting outcome, and then you post that on YouTube and you claim you've done this 100,000 times across the United States, even though you haven't actually done it at all.*[269]
>
> *Then the third scenario that we looked at was conducting a denial of service attack on the Associated Press on Election Day, because pretty much everybody, all those nice maps that everybody puts up on all the different news services, is in fact actually based on Associated Press stringers at all the different precincts and locations. . . . It doesn't actually change anything, but it gives the impression that there's chaos.*[270]

---

[266] (U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 28.

[267] [redacted]

[268] (U) SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 33.

[269] (U) *Ibid.*, pp. 34-35.

[270] (U) *Ibid.*, p. 35.

VI. (U) NO EVIDENCE OF CHANGED VOTES OR MANIPULATED VOTE TALLIES

(U) In its review, the Committee has seen no indications that votes were changed, vote-tallying systems were manipulated, or that any voter registration data was altered or deleted, although the Committee and IC's insight is limited. Poll workers and voting monitors did not report widespread suspicious activity surrounding the 2016 election. DHS Assistant Secretary Jeanette Manfra said in the Committee's open hearing in June 2017 that "I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient." Further, all three witnesses in that hearing—Ms. Manfra, Dr. Liles, and FBI Assistant Director for Counterintelligence Bill Priestap—agreed that they had no evidence that votes themselves were changed in any way in the 2016 election.[271]

- **(U)** Dr. Liles said that DHS "assessed that multiple checks and redundancies in U.S. election infrastructure, including diversity of systems, non-internet connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit, and validate the results—all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected."[272] He later said "the level of effort and scale required to change the outcome of a national election would make it nearly impossible to avoid detection."[273]
- [redacted]
- **(U)** States did not report either an uptick in voters showing up at the polls and being unable to vote or a larger than normal quantity of provisional ballots.

(U) The Committee notes that nationwide elections are often won or lost in a small number of precincts. A sophisticated actor could target efforts at districts where margins are already small, and disenfranchising only a small percentage of voters could have a disproportionate impact on an election's outcome.

(U) Many state election officials emphasized their concern that press coverage of, and increased attention to, election security could create the very impression the Russians were seeking to foster, namely undermining voters' confidence in election integrity. Several insisted that whenever any official speaks publicly on this issue, they should state clearly the difference between a "scan" and a "hack," and a few even went as far as to suggest that U.S. officials stop

---

[271] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017.
[272] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[273] **(U)** *Ibid.*, p. 47.

talking about the issue altogether. One state official said, "We need to walk a fine line between being forthcoming to the public and protecting voter confidence."[274]

(U) Mr. Brennan described a similar concern in IC and policy discussions:

> *We know that the Russians had already touched some of the electoral systems, and we know that they have capable cyber capabilities. So there was a real dilemma, even a conundrum, in terms of what do you do that's going to try to stave off worse action on the part of the Russians, and what do you do that is going to . . . [give] the Russians what they were seeking, which was to really raise the specter that the election was not going to be fair and unaffected.*[275]

(U) Most state representatives interviewed by the Committee were confident that they met the threat effectively in 2016 and believed that they would continue to defeat threats in 2018 and 2020. Many had interpreted the events of 2016 as a success story: firewalls deflected the hostile activity, as they were supposed to, so the threat was not an issue. One state official told the Committee, "I'm quite confident our state security systems are pretty sound."[276] Another state official stated, "We felt good [in 2016]," and that due to additional security upgrades, "we feel even better today."[277]

(U) However, as of 2018, some states were still grappling with the severity of the threat. One official highlighted the stark contrast they experienced, when, at one moment, they thought elections were secure, but then suddenly were hearing about the threat.[278] The official went on to conclude, "I don't think any of us expected to be hacked by a foreign government."[279] Another official, paraphrasing a former governor, said, "If a nation-state is on the other side, it's not a fair fight. You have to phone a friend."[280]

(U) In the month before Election Day, DHS and other policymakers were planning for the worst-case scenario of efforts to disrupt the vote itself. Federal, state, and local governments created incident response plans to react to possible confusion at the polling places. Mr. Daniel said of the effort: "We're most concerned about the Russians, but obviously we are also concerned about the possibility for just plain old hacktivism on Election Day. . . . The incident response plan is actually designed . . . to help us [plan for] what is the federal government going to do if bad things start to happen on Election Day?"

[redacted] Mr. Daniel added that this was the first opportunity to exercise the process established under Presidential Policy Directive-41. "We asked the various agencies with lead

---

[274] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[275] **(U)** SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 54.
[276] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[277] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[278] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[279] **(U)** *Ibid.*
[280] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

responsibility, all right, give us your Election Day plan." That led to the creation of an Election Day playbook; steps included enhanced watch floor procedures, connectivity between FBI field offices and FBI and DHS, and an "escalation path" if "we needed to get to Lisa [Monaco] or Susan [Rice] in a hurry" on Election Day.[281]

VII. (U) SECURITY OF VOTING MACHINES

(U) The Committee review of Russian activity in 2016 highlighted potential vulnerabilities in many voting machines, with previous studies by security researchers taking on new urgency and receiving new scrutiny. Although researchers have repeatedly demonstrated it is possible to exploit vulnerabilities in electronic voting machines to alter votes,[282] some election officials dispute whether such attacks would be feasible in the context of an actual election.

- **(U)** Dr. Alex Halderman, Professor of Computer Science at the University of Michigan, testified before the Committee in June 2017 that "our highly computerized election infrastructure is vulnerable to sabotage and even to cyber attacks that could change votes."[283] Dr. Halderman concluded, "Voting machines are not as distant from the internet as they may seem."[284]

- **(U)** When State 7 decommissioned its Direct-Recording Electronic (DRE) voting machines in 2017, the IT director led an exercise in attempting to break into a few of the machines using the access a "normal" voter would have in using the machines.[285] The results were alarming: the programmed password on some of the machines was ABC123, and the testers were able to flip the machines to supervisor mode, disable them, and "do enough damage to call the results into question."[286] The IT director shared the results with State 21 and State 24, which were using similiar machines.[287]

- **(U)** In 2017, DEFCON[288] researchers were able to find and exploit vulnerabilities in five different electronic voting machines.[289] The WinVote machines, those recently decertified by State 7, were most easily manipulated. One attendee said, "It just took us a couple of hours on Google to find passwords that let us unlock the administrative

---

[281] **(U)** *Ibid.*, p. 82.
[282] **(U)** *See also, infra,* "Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities."
[283] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 117.
[284] **(U)** *Ibid.*, p. 110.
[285] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[286] **(U)** *Ibid.* The machines used were WinVote voting machines.
[287] **(U)** *Ibid.*
[288] **(U)** DEFCON is an annual hacker conference held in Las Vegas, Nevada. In July 2017, at DEFCON 25, the conference featured a Voting Machine Hacking Village ("Voting Village") which acquired and made available to conference participants over 25 pieces of election equipment, including voting machines and electronic poll books, for generally unrestricted examination for vulnerabilities.
[289] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, pp. 8-13.

functions on this machine."[290] A researcher was able to hack into the WinVote over WiFi within minutes using a vulnerability from 2003.[291] Once he had administrator-level access, he could change votes in the database. Researchers also discovered available USB ports in the machine that would allow a hacker to run software on the machine.[292] One said "with physical access to back [sic] of the machine for 15 seconds, an attacker can do anything."[293] Hackers were less successful with other types of machines, although each had recorded vulnerabilities.[294]

- **(U)** The 2018 DEFCON report found similar vulnerabilities, in particular when hackers had physical access to the machines. For example, hackers exploited an old vulnerability on one machine, using either a removable device purchasable on eBay or remote access, to modify vote counts.[295]

- **(U/[redacted])** DHS briefed the Committee in August 2018 that these results were in part because the hackers had extended physical access to the machines, which is not realistic for a true election system. Undersecretary Krebs also disagreed with reporting that a 17-year-old hacker had accessed voter tallies.[296] Some election experts have called into question the DEFCON results for similar reasons and pointed out that any fraud requiring physical access would be, by necessity, small scale, unless a government were to deploy agents across thousands of localities.

- **(U)** ES&S Voting Systems disclosed that some of its equipment had a key security vulnerability. ES&S installed remote access software on machines it sold in the mid-2000s, which allowed the company to provide IT support more easily, but also created potential remote access into the machines. When pressed by Senator Ron Wyden of Oregon, the company admitted that around 300 voting jurisdictions had the software. ES&S says the software was not installed after 2007, and it was only installed on election-management systems, not voting machines.[297] More than 50 percent of voters vote on ES&S equipment, and 41 states use its products.

---

[290] **(U)** Elizabeth Wise, "Hackers at DefCon Conference Exploit Vulnerabilities in Voting Machines," *USA Today*, July 30, 2017, https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/.
[291] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, p. 4.
[292] **(U)** *Ibid.*, p. 9.
[293] **(U)** *Ibid.*
[294] **(U)** *Ibid.*, pp. 8-13.
[295] **(U)** Robert McMillian and Dustin Volz, "Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds," *Wall Street Journal*, September 27, 2018. The machine referenced is the ES&S Model 650, which ES&S stopped making in 2008 but is still available for sale.
[296] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018
[297] **(U)** Hacks, Security Gaps And Oligarchs: The Business of Voting Comes Under Scrutiny. Miles Parks, NPR, September 21, 2018.

(U) Advocates of electronic voting point out the flaws in paper ballots, like the potential for the introduction of fraudulent ballots or invalidated votes due to stains or extra marks. The Committee believes that any election system should be protected end-to-end, including against fraud.

(U) Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities

(U) While best practices dictate that electronic voting machines not be connected to the internet, some machines are internet-enabled. In addition, each machine has to be programmed before Election Day, a procedure often done either by connecting the machine to a local network to download software or by using removable media, such as a thumb drive. These functions are often carried out by local officials or contractors. If the computers responsible for writing and distributing the program are compromised, so too could all voting machines receiving a compromised update. Further, machines can be programmed to show one result to the voter while recording a different result in the tabulation. Without a paper backup, a "recount" would use the same faulty software to re-tabulate the same results, because the primary records of the vote are stored in computer memory.[298]

(U) Dr. Halderman said in his June 2017 testimony before SSCI:

> *I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.*
>
> *Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at the time the most widely used touch-screen DRE in the country and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win.*[299]

---

[298] **(U)** "Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots." Written Statement by J. Alex Halderman, June 21, 2017, citing S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots," *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop,* August 2007; B. Campbell and M. Byrne, "Now do Voters Notice Review Screen Anomalies?" *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop,* August 2009.

[299] **(U)** The machine was the Diebold AccuVote TS, which was still used statewide in at least one state as of 2017.

> *Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in* every single case, *they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes. That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk.*[300]

(U) In speaking with the Committee, federal government officials revealed concerns about the security of voting machines and related infrastructure. Former Assistant Attorney General for National Security John Carlin told the Committee:

> *"I'm very concerned about . . . our actual voting apparatus, and the attendant structures around it, and the cooperation between some states and the federal government."*[301] *Mr. Carlin further stated, "We've literally seen it already, so shame on us if we can't fix it heading into the next election cycles. And it's the assessment of every key intel professional, which I share, that Russia's going to do it again because they think this was successful. So we're in a bit of a race against time heading up to the two-year election. Some of the election machinery that's in place should not be."*[302]

(U) Mr. McCabe echoed these concerns, and noted that, in the last months before the election, FBI identified holes in the security of election machines, saying "there's some potential there."[303]

(U) As of November 2016, five states were using exclusively DRE voting machines with no paper trail, according to open source information.[304] An additional nine states used at least some DRE voting machines with no paper trail.[305]

- **(U)** State 20 has 21-year-old DRE machines. While the state is in the process of replacing its entire voting system, including these machines, State 20 is aiming to have the updates ready for the 2020 elections.

- **(U)** In State 21, 50 of 67 counties as of November 2017 used DRE voting machines.[306]

---

[300] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, pp. 116-117.
[301] **(U)** SSCI Transcript of the Interview with John Carlin, Former Assistant Attorney General for National Security, held on Monday, September 25, 2017, p. 86.
[302] **(U)** *Ibid.*, pp. 86-87.
[303] **(U)** DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, p. 221.
[304] **(U)** BallotPedia, *Voting Methods and Equipment By State*, https://ballotpedia.org/Voting_methods_and_equipment_by_state.
[305] **(U)** *Ibid.*
[306] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.

- **(U)** State 5 used paper-backed voting in only about half its machines and DRE voting machines without paper backup in the other half.[307]

- **(U)** Some states are moving to a hybrid model—an electronic voting machine with a paper backup, often in the form of a receipt that prints after the voter submits their vote. For example, State 12 uses some DREs, but all equipment is required to have a paper trail, and the paper ballot is the ballot of record.[308] State 12 also conducts a mandatory state-wide audit.[309] Similarly, State 13 uses some paper-based and some electronic machines, but all are required to have a paper trail.[310]

(U) The number of vendors selling voting machines is shrinking, raising concerns about a vulnerable supply chain. A hostile actor could compromise one or two manufacturers of components and have an outsized effect on the security of the overall system.

- [redacted] "My job," said Ms. Monaco when asked whether she was worried about voting machines themselves getting hacked, "was to worry about every parade of horribles. So I cannot tell you that that did not cross my mind. We were worried about who, how many makers. We were worried about the supply chain for the voting machines, who were the makers? . . . Turns out I think it's just Diebold—and have we given them a defensive briefing? So to answer your question, we were worried about it all."[311]

- [redacted] Mr. McCabe pointed out that a small number of companies have "90%" of the market for voting machines in the U.S. Before the 2016 election, [redacted] briefed a few of the companies on vulnerabilities,[312] but a more comprehensive campaign to educate vendors and their customers is warranted.

(U) Voluntary Voting System Guidelines

(U) Part of the voting reform implemented under The Help America Vote Act of 2002 was a requirement that the Election Assistance Commission create a set of specifications and requirements against which voting systems can be tested, called the Voluntary Voting System Guidelines (VVSG). The EAC adopted the first VVSG in December 2005. The EAC then tasked the Technical Guidelines Development Committee, chaired by the National Institute of Standards and Technology (NIST) and including members from NASED, with updating the guidelines. In March 2015, the EAC approved VVSG 1.1; in January 2016, the EAC adopted

---

[307] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.
[308] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[309] **(U)** *Ibid.*
[310] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[311] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 31.
[312] **(U)** SSCI Transcript of the Interview with Andy McCabe, Deputy Director of the FBI, held on Wednesday, February 14, 2018, pp. 220-221.

an implementation plan requiring that all new voting systems be tested against the VVSG 1.1 beginning in July 2017. VVSG 1.1 has since been succeeded by version 2.0, which was released for a 90-day public comment period on February 15, 2019. The EAC will compile the feedback for Commissioners to review shortly thereafter.[313] VVSG 2.0 includes the following minimum security guidelines:

- **(U)** An error or fault in the voting system software or hardware cannot cause an undetectable change in election results. (9.1)
- **(U)** The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities. (9.2)
- **(U)** Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. (9.3)
- **(U)** The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. (11.3)
- **(U)** The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. (13.1)
- **(U)** The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls. (14.2)
- **(U)** The voting system employs mechanisms to protect against malware. (15.3)
- **(U)** A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice. (15.4)

(U) As of March 2018, 35 states required that their machines be certified by EAC, but compliance with the VVSG standards is not mandatory. Secretary Nielsen testified before the Committee that the United States should "seek for all states" to use the VVSG standards.[314]

---

[313] **(U)** *EAC Commissioners Unanimously Vote to Publish VVSG 2.0 Principles and Guidelines for Public Comment;* https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/; February 15, 2019

[314] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 47.

VIII. (U) THE ROLE OF DHS AND INTERACTIONS WITH THE STATES

(U) The federal government's actions to address election security threats evolved significantly from the summer of 2016 through the summer of 2018. Contemporaneous with the Russian attacks, DHS and FBI were initially treating the situation as they would a typical notification of a cyber incident to a non-governmental victim. By the fall of 2016, however, DHS was attempting to do more extensive outreach to the states. Then in the fall of 2017, DHS undertook an effort to provide a menu of cyber support options to the states.

A. (U) DHS's Evolution

[redacted] For DHS and other agencies and departments tasked with intelligence collection or formulating policy options through the interagency process, the full scope of the threat began to emerge in the summer of 2016. Secretary Johnson told the Committee that "I know I had significant concerns by [summer of 2016] about doing all we could to ensure the cybersecurity of our election systems."[315] Mr. Daniel said in his interview that by the end of July, the interagency was focused on better protecting electoral infrastructure as part of a "DHS and FBI-led domestic effort."[316]

[redacted] Policymakers quickly realized, however, that DHS was poorly positioned to provide the kind of support states needed. Mr. Daniel said that interagency discussions about the threat "start[ed] a process of us actually realizing that, frankly, we don't actually have very much in the way of capability that we can directly offer the states"—a fact that the states themselves would later echo.[317]

- [redacted] Ms. Monaco said that DHS initially found a "pretty alarming variance in the number of voting registration databases and lack of encryption and lack of backup for all of these things."[318] Ms. Monaco added that "[i]n light of what we were seeing, in light of the intelligence we were getting briefed on, this was a very specific direction and decision to say we need to really accelerate this, put a significant push on resources and engagement at the senior-most levels."[319]

- [redacted] Mr. Daniel and the working group identified DHS's cyber teams as possible assistance to the states. "DHS had teams that could go and provide that support to the private sector. We've been doing that. That's a program that existed for years for critical

---

[315] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[316] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 28.
[317] **(U)** *Ibid.*, p. 38.
[318] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 19.
[319] **(U)** *Ibid.*, p. 21.

infrastructure companies. And we realized that we could repurpose [some of those teams], but we don't have that many of them . . . four or five. It was not very many." [320]

(U) DHS attempted a nuanced outreach to the states on the threat. Ms. Monaco highlighted a delicate balancing act with the interactions with states:

> *I know we tried very hard to strike a balance between engaging state and local officials and federal officials in the importance of raising cyber defenses and raising cybersecurity . . . and not sowing distrust in the system, both because, one, we believed it to be true that the system is in fact quite resilient because of what I mentioned earlier, which is the diffuse nature; and because we did not want to, as we described it, do the Russians' work for them by sowing panic about the vulnerability of the election.*[321]

(U) In an August 15, 2016, conference call with state election officials, then-Secretary Johnson told states, "we're in a sort of a heightened state of alertness; it behooves everyone to do everything you can for your own cybersecurity leading up to the election." He also said that there was "no specific or credible threat known around the election system itself. I do not recall—I don't think, but I do not recall, that we knew about [State 4] and Illinois at that point."[322] The Committee notes that this call was two months after State 4's system was breached, and more than a month after Illinois was breached and the state shut down its systems to contain the problem. During this call, Secretary Johnson also broached the idea of designating election systems as critical infrastructure.

(U) A number of state officials reacted negatively to the call. Secretary Johnson said he was "surprised/disappointed that there was a certain level of pushback from at least those who spoke up. . . . The pushback was: This is our—I'm paraphrasing here: This is our responsibility and there should not be a federal takeover of the election system."[323]

- **(U)** The call "does not go incredibly well," said Mr. Daniel. "I was not on the call, no, but all of the reporting back and then all of the subsequent media reporting that is leaked about the call shows that it did not go well." Mr. Daniel continued: "I was actually quite surprised . . . in my head, there is this: yes, we have this extremely partisan election going on in the background; but the Russians are trying to mess with our election. To me, that's a national security issue that's not dependent on party or anything else."[324]

---

[320] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 41.
[321] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 29.
[322] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 13.
[323] **(U)** *Ibid.*, pp. 13-14.
[324] **(U)** *Ibid.*, p. 48.

- **(U)** Ms. Monaco also related how DHS received significant push back from the states and decided to "focus our efforts on really pushing states to voluntarily accept the assistance that DHS was trying to provide."[325]

- **(U)** States also reported that the call did not go well. Several states told the Committee that the idea of a critical infrastructure designation surprised them and came without context of a particular threat. Some state officials also did not understand what a critical infrastructure designation meant, in practical terms, and whether it would give the federal government the power to run elections. DHS also did not anticipate a certain level of suspicion from the states toward the federal government. As a State 17 official told the Committee, "when someone says 'we're from the government and we're here to help,' it's generally not a good thing."[326]

(U) Critical Infrastructure Designation

(U) One of the most controversial elements of the relationship between DHS and the states was the decision to designate election systems as critical infrastructure. Most state officials relayed that they were surprised by the designation and did not understand what it meant; many also felt DHS was not open to input from the states on whether such a designation was beneficial.

(U) Secretary Johnson remembers the first time he aired the possibility of a designation was on August 3, 2016. He went to a reporters' breakfast sponsored by the Christian Science Monitor and publicly "floated the idea of designating election infrastructure as critical infrastructure."[327] Then, on August 15, 2016, Secretary Johnson had a conference call with election officials from all 50 states. "I explained the nature of what it means to be designated critical infrastructure. It's not a mandatory set of [regulations], it's not a federal takeover, it's not binding operational directives. And here are the advantages: priority in terms of our services and the benefit of the protection of the international cyber norm."[328] Secretary Johnson continued: "I stressed at the time that this is all voluntary and it prioritizes assistance if they seek it."[329]

(U) Some states were vocal in objecting to the idea. In evaluating the states' response, DHS came to the conclusion that it should put the designation on hold, deciding it would earn more state trust and cooperation if it held off on the designation as critical infrastructure and perhaps sought more buy-in from the states at a later date.[330]

---

[325] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 25.
[326] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018.
[327] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[328] **(U)** *Ibid.*, p. 14. For additional information on the definition of critical infrastructure in a cybersecurity context, *see* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.
[329] **(U)** SSCI Transcript of the Open Hearing on Election Security, March 21, 2018, p. 34.
[330] **(U)** *Ibid.*, p. 115.

(U) After the election, Secretary Johnson decided the time had come to make the designation. He held a follow-up call with NASS on the critical infrastructure designation in January 2017: "I didn't tell them I'm doing this the next day, but I told them I was close to making a decision. I didn't hear anything further [along the lines of additional, articulated objections], so the same day we went public with the [unclassified] version of the report,[331] I also made the designation."[332]

(U) Mr. Daniel summed up the rationale for proceeding this way: "I do believe that we should think of the electoral infrastructure as critical infrastructure, and to me it's just as critical for democracy as communications, electricity, water. If that doesn't function, then your democracy doesn't function. . . . To me that is the definition of 'critical.'"[333]

(U) In interviews with the Committee in late 2017 and early 2018, several states were supportive of the designation and saw the benefits of, for example, the creation of the Government Coordinating Council. Others were lukewarm, saying they had seen limited benefits for all the consternation officials said it had caused. Still others remained suspicious that the designation is a first step toward a federal takeover of elections.

B. (U) The View From the States

(U) For most states, the story of Russian attempts to hack state infrastructure was one of confusion and a lack of information. It began with what states interpreted as an insignificant event: an FBI FLASH notification on August 18, 2016, [redacted][334] Then, in mid-October, the MS-ISAC reached out to state IT directors with an additional alert about specific IP addresses scanning websites.[335] At no time did MS-ISAC or DHS identify the IP addresses as associated with a nation-state actor. Given the lack of context, state staff who received the notification did not ascribe any additional urgency to the warning; to them, it was a few more suspect IP addresses among the thousands that were constantly pinging state systems. Very few state IT directors informed state election officials about the alert.

---

[331] **(U)** Secretary Johnson was referring to the declassified version of the Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections,* January 6, 2017.
[332] **(U)** *Ibid.*, p. 46.
[333] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 98.
[334] **(U)** FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER, [redacted]
[335] **(U)** FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems,* October 14, 2016.

- **(U)** State 11 had a meeting with DHS officials, including the regional DHS cyber advisor, in August 2016, but according to State 11 officials, DHS did not mention any specific threat against election systems from a nation-state actor.[336]

- **(U)** State 13 reported that DHS contacted an affected county at one point, but never contacted the state-level officials.[337]

- **(U)** When they saw an IP address identified in the alerts had scanned their systems, State 6 and State 16 sent their logs to the MS-ISAC for analysis.[338] State 16 said it never received a response.[339]

(U) DHS, conversely, saw its efforts as far more extensive and effective. Ms. Manfra testified to SSCI that DHS "held a conference call where all 50 secretaries of state or an election director if the secretary of state didn't have that responsibility [participated], in August, in September, and again in October [of 2016], both high-level engagement and network defense products [sic]."[340] Mr. Daniel reported that "by the time Election Day rolls around, all but one state has taken us up on the offer to at least do scanning [,] so I want to give people credit for not necessarily sticking to initial partisan reactions and . . . taking steps to protect their electoral infrastructure."[341]

(U) States reported to the Committee that Election Day went off smoothly. For most state election officials, concerns about a possible threat against election systems dropped off the radar until the summer or fall of 2017. Many state election officials reported hearing for the first time that Russian actors were responsible for scanning election infrastructure in an estimated 21 states from the press or from the Committee's open hearing on June 21, 2017. During that hearing, in response to a question from Vice Chairman Warner inquiring whether all affected states were aware they were attacked, Ms. Manfra responded that "[a]ll of the system owners within those states are aware of the targeting, yes, sir."[342] However, when pressed as to whether election officials in each state were aware, the answer was less clear.[343]

- **(U)** In that hearing, Dr. Liles said DHS had "worked hand-in-hand with the state and local partners to share threat information related to their networks."[344]

---

[336] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[337] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[338] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[339] **(U)** *Ibid.* State 6 did not indicate whether they received feedback from DHS.
[340] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, June 21, 2017, p. 74.
[341] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 49.
[342] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 28.
[343] **(U)** *Ibid.*, pp. 62-63.
[344] **(U)** *Ibid.*, p. 12.

- **(U)** Ms. Manfra said, "The owners of the systems within those 21 states have been notified." Senator King then asked, "How about the election officials in those states?" Ms. Manfra responded, "We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states ....[crosstalk]."[345]

- **(U)** Given Ms. Manfra's testimony and the fact that some election officials did not get a notification directly to their offices, election officials in many states assumed they were not one of the 21; some even issued press releases to that effect.[346]

(U) The disconnect between DHS and state election officials became clear during Committee interactions with the states throughout 2017. In many cases, DHS had notified state officials responsible for network security, but not election officials, of the threat. Further, the IT professionals contacted did not have the context to know that this threat was any different than any other scanning or hacking attempt, and they had not thought it necessary to elevate the warning to election officials.

(U) After the hearing, and in part to respond to confusion in the states, DHS held a conference call with representatives from 50 states in September 2017. In that call, DHS said they would contact affected states directly. State 8 state election officials noted that the call became "somewhat antagonistic."[347] State 17 officials reported that the phone call "just showed how little DHS knew about elections."[348] Several officials argued that all 50 states should be notified of who had been hacked. DHS followed up with one-to-one phone calls to states over the next several days.

- **(U)** Officials from some states reported being shocked that they were in fact one of the states, and further surprised that their states had supposedly been notified.

- **(U)** Most state officials found the conference calls lacking in information and were left wondering exactly what the threat might be. Several states said the DHS representatives could not answer any specific questions effectively.

(U) Following this series of difficult engagements, DHS set about trying to build relationships with the states, but it faced a significant trust deficit. Early follow-up interactions between state election officials and DHS were rocky. States reported that DHS seemed to have little to no familiarity with elections. For example, State 6 said that the DHS representatives they were assigned seemed to know nothing about State 6, and, when pressed, they admitted they were "just reading the spreadsheet in front of [them]."[349] State 8 reported that "we are spending

---

[345] **(U)** *Ibid.*, pp. 62-63.
[346] **(U)** State 8 said they put out a press release because DHS had said publicly that they had notified the 21 states, and "if you were one of the 21, you would know."
[347] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[348] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[349] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.

a ton of time educating outside groups on how elections are run."[350] State 3 officials said, "DHS didn't recognize that securing an election process is not the same as securing a power grid."[351]

(U) By early 2018, State officials gave DHS credit for making significant progress over the next six months. States began to sign up for many of the resources that DHS had to offer, and DHS hosted the first meeting of the Government Coordinating Council required under the critical infrastructure designation. Those interactions often increased trust and communication between the federal and state entities. For example, DHS has identified a list of contacts to notify if they see a threat; that list includes both IT officials and election officials. State 9 described it as "quite a turnaround for DHS," and further stated that the Secretaries of State had been disappointed with how slowly DHS got up to speed on election administration and how slowly the notifications happened, but DHS was "quick with the *mea culpas* and are getting much better." [352]

(U) Not all of the engagements were positive, however. State 13 in early December 2017 still reported continued frustration with DHS, indicating to the Committee that it had not seen much change in terms of outreach and constructive engagement. As of summer 2017, according to State 13, "the lack of urgency [at DHS] was beyond frustrating."[353]

C. (U) Taking Advantage of DHS Resources

(U) As DHS has pursued outreach to the states, more and more have opened their doors to DHS assistance. DHS told the Committee that its goal has been relationship building and:

> *In the partnerships with the states and secretaries of states, state election directors, and at the local level, we're trying to shift them to a culture of more information security management, where they can now account for the integrity of their system, or, if something did happen . . . they know the full extent of what happened on their system. . . . We're providing vulnerability assessments and trend analysis, in addition to connecting them to the threat intelligence that we can, in order to evolve their . . . cyber culture.* [354]

(U) DHS's assistance can be highly tailored to need, and falls into roughly two buckets: remote cyber hygiene scans, which provide up to weekly reports, and on-site risk and vulnerability assessments. DHS also offers a suite of other services, including phishing campaign assessments. All these efforts seek to provide the states with actionable information to improve cyber hygiene, but DHS has been keen to avoid what could be perceived by the states as

---

[350] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[351] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.
[352] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[353] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[354] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, pp. 54-55.

unfunded mandates.[355] Some states requesting more intensive services have also experienced significant delays before DHS could send a team to assist.

- **(U)** By October 2018, DHS said 35 states, 91 local jurisdictions, and eight election system vendors had signed up for remote persistent scans.[356] All the requests for these scans have been fulfilled. "They can be turned on basically within the week," according to DHS.[357]

- **(U)** DHS said that as of October 2018, it had completed 35 in-depth, on the ground vulnerability assessments: 21 states, 13 localities, and one election system vendor. These assessments are one week off-site remote scans followed by a second week on site.[358]

- **(U)** Two states who completed the in-depth assessments reported in late 2017 they had had a good experience. State 12 officials said the team was "extremely helpful and professional."[359] State 10 said the review was a good experience, although DHS was somewhat limited in what it could do.[360] For example, DHS did a phishing email test that showed the training for employees had worked.[361] DHS gave "good and actionable recommendations." Although DHS "didn't really understand election systems when they came," they learned a lot.[362]

- **(U)** As of November 2017, State 6 and State 9 requested an on-site scan, but those scans were on track to be delayed past the August 2018 primaries.[363] State 7 was expecting a four-to-six month delay.[364] State 8 signed up for a checkup in October 2017 and was due to get service the following February.[365] As of January 2018, State 17 also had requested an on-site scan.[366]

(U) In a sign of improving relations between the states and DHS, two states that had elections in 2017 attempted to include DHS in the process more extensively than in the past. In State 17, a two-person DHS team sat with election officials during the 2017 special election and monitored the networks. Even though "their presence was comforting," they "really didn't do much." State 17 signed DHS's normal MOU, but also added its own clause to underscore the state's independence: a formal sunset on DHS's access to state systems, one week after the

---

[355] **(U)** *Ibid.*, p. 60.
[356] **(U)** *Ibid.*, p. 57.
[357] **(U)** DHS phone call with SSCI; October 16, 2018.
[358] **(U)** *Ibid.*
[359] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[360] **(U)** *Ibid.*
[361] **(U)** *Ibid.*
[362] **(U)** *Ibid.*
[363] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[364] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[365] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[366] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.

election. State 7 reported their experience with DHS during the 2017 statewide election was quite good. DHS sat with election officials all day, which meant State 7 could pass messages quickly to NCCIC.

(U) In March 2018, Congress appropriated $380 million in funding for election security improvements. The funding was distributed under the formula laid out in the Help American Vote Act (HAVA) and was intended to aid in replacing vulnerable voting machines and improving cybersecurity. As of July 2018, 13 states said they intended to use the funds to buy new voting machines, and 22 said they have "no plans to replace their machines before the election—including all five states that rely solely on paperless electronic voting devices," according to a survey by Politico.[367]

IX. (U) RECOMMENDATIONS

1. (U) Reinforce States' Primacy in Running Elections*

(U) States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.

2. (U) Build a Stronger Defense, Part I: Create Effective Deterrence

(U) The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act, and we will respond accordingly. The U.S. Government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator.

[redacted] **Ideally, this principle of deterrence should be included in an overarching cyber doctrine for the U.S. Government**. That doctrine should clearly delineate cyberespionage, cybercrime, and cyber attacks. Further, a classified portion of the doctrine should establish what the U.S. Government believes to be its escalation ladder in the cyber realm—what tools does it have, what tools should it pursue, and what should the limits of cyber war be. The U.S. strategic approach tends to overmatch adversaries with superior technology, and policymakers should consider what steps the U.S. will need to take to outstrip the capabilities of Russia, China, Iran, North Korea, and other emerging hostile actors in the cyber domain.

(U) U.S. cyber doctrine should serve as the basis for a discussion with U.S. allies and others about new cyber norms. Just as the international community has established norms and treaties about the use of technologies and weapons systems, the U.S. should lead a conversation about cyber norms and the limits of cyber activity with allies and others.

*The Committee's recommendation to "reinforce states' primacy in running elections" should be understood in reference to states' responsibility for election security, and not as pertaining to broader election issues, such as campaign finance laws or voting rights laws.

[367] **(U)** States Slow to Prepare for Hacking Threats, Eric Geller, Politico, July 18, 2018.

3. (U) Build a Stronger Defense, Part II: Improve Information Gathering and Sharing on Threats

[redacted]

[redacted] **The U.S. government needs to build the cyber expertise and capacity of its domestic agencies, such as DHS and FBI, and reevaluate the current authorities that govern efforts to defend against foreign cyber threats.** NSA and CIA collection is, by law, directed outside the United States. [redacted]

[redacted] **The U.S. government should invest in capabilities for rapid attribution of cyber attacks, without sacrificing accuracy.** [redacted] However, the IC needs to improve its ability to provide timely and actionable warning. Timely and accurate attribution is not only important to defensive information sharing, but will also underpin a credible deterrence and response strategy.

(U) The federal government and state governments need to create clear channels of communication two ways—down from the federal government to the state and local level, and up from the state and local officials on the front lines to federal entities. In 2016, DHS and FBI did not provide enough information or context to election officials about the threat they were facing, but states and DHS have made significant progress in this area in the last two years. For example, Secretary of Homeland Security Nielsen testified to the Committee in March 2018 that "today I can say with confidence that we know whom to contact in every state to share threat information. That capability did not exist in 2016."[369]

(U) A key component of information sharing about elections is security clearances for appropriate officials at the state and local level. DHS and its partners can effectively strip classified information off of cyber indicators, which can then be passed to technical staff at the state level, but in order for those indicators to not get lost in the multitude of cyber threats those professionals see on a daily basis, senior officials at the state and local levels need to know the

---

[368] [redacted]

[369] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 16.

context surrounding the indicators. State officials need to know why a particular threat is of significant concern, and should be prioritized. That context could come from classified information, or states could come to understand that threat information DHS passes them is more serious than that received through other sources. DHS's goal is to obtain clearances for up to three officials per state.[370] As of August 2018, DHS had provided a clearance to 92 officials[371]; as of late 2017 all state election officials had received interim secret clearances or one-day read-ins for secret-level briefings.[372] DHS, along with ODNI and FBI, also hosted state and local election officials for a SECRET-level briefing on the sidelines of the biannual NASS and NASS-ED conferences in Washington, DC in February 2018. In March, Amy Cohen, Executive Director of NASS-ED testified in front of the Committee that, "It would be naïve to say that we received answers to all our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community as well as to our concerns."[373] The Committee recommends DHS continue providing such briefings and improve the quality of information shared.

(U) Fundamental to meaningful information sharing, however, is that state officials understand what they are getting. New inductees to the world of classified information are often disappointed—they expected to see everything laid out in black and white, when intelligence is often very gray, with a pattern discernable only to those who know where to look and what conclusions to draw. Those sharing the intelligence should manage expectations—at the SECRET level, officials are likely to see limited context about conclusions, but not much more.

(U) Federal officials should work to declassify information, for the purpose of providing warning to appropriate state and local officials, to the greatest extent possible. If key pieces of context could be provided at a lower classification level while still protecting classified information, DHS and its partners should strive to do so.

4. (U) Build a Stronger Defense, Part III: Secure Election-Related Cyber Systems

(U) Despite the expense, cybersecurity needs to become a higher priority for election-related infrastructure. The Committee found a wide range of cybersecurity practices across the states. Some states were highly focused on building a culture of cybersecurity; others were severely under-resourced and relying on part-time help.

(U) The Committee recommends State officials work with DHS to evaluate the security of their election systems end-to-end and prioritize implementing the following steps to secure voter registration systems, state records, and other pre-election activities. The Committee additionally recommends that State officials:

---

[370] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.15.
[371] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[372] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p 15, 26.
[373] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.113.

- **(U)** Identify the weak points in their networks, like under-resourced localities. State 7 said they are not worried about locations like larger counties when it comes to network security, but they are worried about "the part-time registrar who is also the town attorney and the town accountant and is working out of a 17th century jail." [374]

- **(U)** Undertake security audits of state and local voter registration systems, ideally utilizing private sector entities capable of providing such assistance. State and local officials should pay particular attention to the presence of high severity vulnerabilities in relevant web applications, as well as highly exploitable vulnerabilities such as cross-site scripting and SQL injection.

- **(U)** Institute two-factor authentication for user access to state databases.

- **(U)** Install monitoring sensors on state systems. As of mid-2018, DHS's ALBERT sensors covered up to 98% of voting infrastructure nationwide, according to Undersecretary Krebs.[375]

- **(U)** Include voter registration database recovery in state continuity of operations plans.

- **(U)** Update software in voter registration systems. One state mentioned that its voter registration system is more than ten years old, and its employees will "start to look for shortcuts" as it gets older and slower, further imperiling cybersecurity.

- **(U)** Create backups, including paper copies, of state voter registration databases.

- **(U)** Consider a voter education program to ensure voters check registration information well prior to an election.

(U) DHS in the past year has stepped up its ability to assist the states with some of these activities, but DHS needs to continue its focus on election infrastructure and pushing resources to the states.

(U) The Committee recommends DHS take the following steps:

- **(U)** Create an advisory panel to give DHS expert-level advice on how states and localities run elections. The Government Coordinating Council, created as part of the critical infrastructure designation, could serve as a venue for educating DHS on what states do and what they need.

---

[374] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[375] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

- **(U)** Create guidelines on cybersecurity best practices for elections and a public awareness campaign to promote election security awareness, working through EAC, NASS, and NASED, and with the advisory panel.

- **(U)** Develop procedures and processes to evaluate and routinely provide guidance on relevant vulnerabilities associated with voting systems in conjunction with election experts.

- **(U)** DHS has already created a catalog of services they can provide to states to help secure states' systems. DHS should maintain the catalog and continue to update it as it refines its understanding of what states need.

- **(U)** Expand capacity so wait times for services, like voluntary vulnerability assessments, are manageable and so that DHS can maintain coverage on other critical infrastructure sectors. Robbing resources from other critical infrastructure sectors will eventually create unacceptable new vulnerabilities.

- **(U)** Work with GSA to establish a list of approved private-sector vendors who can provide services similar to those DHS provides. States report being concerned about "vultures" —companies who show up selling dubious cyber solutions. That being said, some states will be more comfortable having a private sector entity evaluate their state systems than a federal agency.

- **(U)** Continue to build the resources of the newly established EI-ISAC. States have already found this information sharing service useful, and it could serve as a clearinghouse for urgent threat information. As of August 2018, the EI-ISAC had over 1,000 members with participants in all 50 states.[376]

- **(U)** Continue training for state and local officials, like the table-top exercise conducted in August of 2018 that brought together representatives from 44 states, localities, and the federal government to work through an election security crisis.[377] The complexity of the scenario encouraged state and local officials to identify serious gaps in their preparations for Election Day.

5. (U) Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself

(U) Given Russian intentions to undermine the credibility of the election process, states should take urgent steps to replace outdated and vulnerable voting systems. When safeguarding the integrity of U.S. elections, all relevant elements of the government—including at the federal, state, and local level—need to be forward looking and work to address vulnerabilities before they are exploited.

---

[376] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[377] **(U)** DHS, Press release: DHS Hosts National Exercise on Election Security, August 15, 2018.

- **(U)** As states look to replace HAVA-era machines that are now out of date, they should purchase more secure voting machines. Paper ballots and optical scanners are the least vulnerable to cyber attack; at minimum, any machine purchased going forward should have a voter-verified paper trail and remove (or render inert) any wireless networking capability.

- **(U)** States should require that machines purchased from this point forward are either EAC certified or comply with the VVSG standards. State purchasers should write contracts with vendors to ensure adherence to the highest security standards and to demand guarantees the supply chains for machines are secure.

- **(U)** In concert with the need for paper ballots comes the need to secure the chain of custody for those ballots. States should reexamine their safeguards against insertion of fraudulent paper ballots at the local level, for example time stamping when ballots are scanned.

- **(U)** Statistically sound audits may be the simplest and most direct way to ensure confidence in the integrity of the vote.[378] States should begin to implement audits of election results. Logic and accuracy tests of machines are a common step, but do not speak to the integrity of the actual vote counting. Risk-limiting audits, or some similarly rigorous alternative, are the future of ensuring that votes cast are votes counted. State 8, State 12, State 21, State 9, State 2, State 16, and others already audit their results, and others are exploring additional pilot programs.[379] However, as of August 2018, five states conducted no post-election audit and 14 states do not do a complete post-election audit.[380] The Committee recognizes states' concern about the potential cost of such audits and the necessary changes to state laws and procedures; however, the Committee believes the benefit of having a provably accurate vote is worth the cost.

- **(U)** States should resist pushes for online voting. One main argument for voting online is to allow members of the military easier access to their fundamental right to vote while deployed. While the Committee agrees states should take great pains to ensure members

---

[378] **(U)** Election experts point out, however, that audits could create a new vector for election-related lawsuits. Complainants could allege that the audit was done improperly, or that the audit process reflected bias.

[379] **(U)** State 8 passed a law to audit starting in 2018, with random precinct sampling. State 12 does state-wide audits. State 21 audits 2% of ballots, randomly selected. State 9 picks 210 of 4100 precincts at random for an audit. State 2 hand-counts ballots in randomly selected precincts and uses automated software to test. A States law on ballot storage can't accommodate risk-limiting audits. Instead, they use ClearBallot software. They upload images of ballots to an external hard drive and send it to ClearBallot. ClearBallot is blind to who won and independently evaluates the results. In addition, the company can identify problems with scanners; for example, when a fold in absentee ballots recorded as a vote. Cybersecurity experts still doubt, however, that this type of procedure is secure.

[380] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

of the military get to vote for their elected officials, no system of online voting has yet established itself as secure.[381]

- **(U)** DHS should work with vendors of election equipment to educate them about the vulnerabilities in both the machines and the supply chains for the components of their machines. Idaho National Lab is already doing some independent work on the security of a select set of voting machines, developing a repeatable methodology for independently testing the security of such systems.

- **(U)** The Department of State should work with FBI and DHS to warn states about foreign efforts to access polling places outside normal channels in the future and remain vigilant about rejecting aberrant attempts.

- **(U)** The Associated Press is responsible for reporting unofficial, initial election results on election night and is a critical part of public confidence in the voting tally. States and DHS should work with the AP and other reporting entities to ensure they are both secure and reporting accurate results.

- **(U)** The Committee found that, often, election experts, national security experts, and cybersecurity experts are speaking different languages. Election officials focus on transparent processes and open access and are concerned about introducing uncertainty into the system; national security professionals tend to see the threat first. Both sides need to listen to each other better and to use more precise language.

6. (U) Assistance for the States

(U) State officials told the Committee the main obstacle to improving cybersecurity and purchasing more secure voting machines is cost. State budgets are stretched thin by priorities that seem more urgent on a daily basis and are far more visible to constituents.

(U) In March 2018, Congress appropriated $380 million in funds under the HAVA formula for the states. As of August 2018, states had begun to allocate and spend that money for items such as cybersecurity improvements.

(U) The Committee recommends the EAC, which administers the grants, regularly report to Congress on how the states are using those funds, whether more funds are needed, and whether states have both replaced outdated voting equipment and improved

---

[381] **(U)** Dr. Halderman in his testimony before the Committee said, "I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would need in order for voters to have high confidence. And I say that having myself . . . hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use." *See* SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 152.

cybersecurity. More funds may be needed, as the allocation under the HAVA formula did not prioritize replacing vulnerable electronic-only machines.

- **(U)** States should be able to use grant funds to improve cybersecurity in a variety of ways, including hiring additional IT staff, updating software, and contracting with vendors to provide cybersecurity services. "Security training funded and provided by a federal entity such as the EAC or DHS would also be beneficial in our view,"[382] an official from Illinois testified.

- **(U)** Funds should also be available to defray the cost of instituting audits.

- **(U)** States with vulnerable DRE machines with no paper backup should receive urgent access to funding. Dr. Halderman testified that replacing insecure paperless voting machines nationwide would cost $130 to $400 million dollars. Risk-limiting audits would cost less than $20 million a year.[383]

7. [redacted] **Build a Credible** [redacted]

[redacted]

[redacted]

[382] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 114.
[383] **(U)** *Ibid.*, p. 119.

MINORITY VIEWS OF SENATOR WYDEN

(U) The role of the federal government

(U) The Committee report describes Russian attacks on U.S. election infrastructure in 2016 and lays out many of the serious vulnerabilities that exist to this day. These vulnerabilities pose a direct and urgent threat to American democracy which demands immediate congressional action. The defense of U.S. national security against a highly sophisticated foreign government cannot be left to state and county officials. For that reason, I cannot support a report whose top recommendation is to "reinforce[ ] state's primacy in running elections."

(U) Congress's constitutional role in regulating federal elections is well-established. In response to an inquiry from the bipartisan leadership of the U.S. Senate, the General Accounting Office (GAO) wrote that "[w]ith regard to the administration of federal elections, Congress has constitutional authority over both congressional and presidential elections."[1] Indeed, pursuant to the Elections Clause of the U.S. Constitution,[2] Congress's authority over congressional elections is "paramount to that of the states." As the GAO report details, Congress has repeatedly passed legislation related to the administration of elections on topics such as the timing of federal elections, voter registration, absentee voting requirements, disability access, and voting rights.

(U) If there was ever a moment when Congress needed to exercise its clear constitutional authorities to regulate elections, this is it. America is facing a direct assault on the heart of our democracy by a determined adversary. We would not ask a local sheriff to go to war against the missiles, planes and tanks of the Russian Army. We shouldn't ask a county election IT employee to fight a war against the full capabilities and vast resources of Russia's cyber army. That approach failed in 2016 and it will fail again. The federal government's response to this ongoing crisis cannot be limited offers to provide resources and information, the acceptance of which is voluntary. If the country's elections are to be defended, Congress must also establish mandatory, nation-wide cybersecurity requirements.

(U) Security of voting machines

(U) Experts are clear about the measures necessary to protect U.S. elections from cyber manipulation.[3] Absent an accessibility need, most voters should hand-mark paper ballots. For voters with some kind of need, ballot marking devices that print paper ballots should be available. Risk-limiting audits must be also be required. Currently, however, only Virginia, Colorado and Rhode Island meet these requirements.[4] These critical reforms must be adopted

---

[1] "Elections. The Scope of Congressional Authority in Election Administration," General Accounting Office, March 2001, prepared in response to a joint inquiry from Senator Trent Lott, Republican Leader; Senator Tom Daschle, Democratic Leader; Senator Mitch McConnell, Chairman, and Senator Christopher Dodd, Ranking Member, of the Senate Committee on Rules and Administration.

[2] Article I, Section 4, Clause 1

[3] Securing the Vote; Protecting American Democracy; National Academy of Sciences, Engineering and Medicine, September 2018

[4] National Conference of State Legislatures, Post-Election Audits, January 3, 2019. Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018. Oregon requires paper ballots and the Oregon State Senate has passed a bill requiring risk-limiting audits.

throughout the country, which is why, on June 27, 2019, the House of Representatives passed H.R. 2722, the Securing America's Federal Elections (SAFE) Act. The security of the country's voting machines depends on this legislation being signed into law.

(U) The Committee, in recommending basic security measures like paper ballots and audits, notes that there is currently "a wide range of cybersecurity practices across the states." Indeed, the data is deeply concerning and highlights the need for mandatory, nation-wide standards. For example, the Committee rightly highlights the vulnerabilities of Direct-Recording Electronic (DRE) Voting Machines, noting that, without a paper trail, there would be no way to conduct a meaningful "recount" and compromises would remain undetected. As of November 2018, however, there were still four states in which every single county relied on DREs without voter verified paper audit trail printers (VVPAT) and, in an additional eight states, there were multiple counties that relied on DREs without a VVPAT.[5] Gaps in the deployment of VVPATs, which are far less secure than hand-marked paper ballots, demonstrate that even bare minimum security best practices are not being met in many parts of the country.

(U) In addition, 16 states have no post-election audits of any kind, while many others have insufficient or perfunctory audits. Only four states have a statutory requirement for risk-limiting audits, while two states provide options for counties to run different kinds of audits, one of which is a risk-limiting audit.[6] Next year, a third state will provide that option. In other words, the vast majority of states have made no moves whatsoever toward implementing minimum standards that experts agree are necessary to guarantee the integrity of elections.

(U) The Committee rightly identifies problems with vendors of voting machines, noting vulnerabilities in both the machines and the supply chains for machine components. Currently, however, the federal government has no regulatory authority that would require these vendors to adhere to basic security practices.[7] Only general federal requirements that states and localities use paper ballots and conduct audits will ensure that the risk posed by voting machines provided by private vendors to states and localities can be contained. The stakes could not be more clear. As Homeland Secretary Kirstjen Nielsen testified to the Committee, "If there is no way to audit the election, that is absolutely a national security concern."[8]

(U) Registration databases and election night reporting websites

(U) Two additional components of the U.S. election infrastructure require immediate, mandatory cybersecurity fixes. The first are voter registration databases. The Committee received testimony about successful Russian exfiltration of databases of tens of thousands of voters.[9] Expert witnesses also described the chaos that manipulated voter registration data could cause should voters arrive at the polls and find that their names had been removed from the rolls.

---

[5] Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018.
[6] The four states are Colorado, Nevada, Rhode Island, and Virginia. National Conference of State Legislatures, Post-Election Audits, January 3, 2019.
[7] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.
[8] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.
[9] Testimony of Connie Lawson, President-elect, National Association of Secretaries of State, and Secretary of State, State of Indiana; testimony of Steve Sandvoss, Executive Director of Illinois State Board of Elections, June 21, 2017; Illinois Voter Registration System Database Breach Report.

As one expert testified, this form of interference "could be used to sabotage the election process on Election Day."[10]

(U) The Committee report describes a range of cybersecurity measures needed to protect voter registration databases, yet there are currently no mandatory rules that require states to implement even minimum cybersecurity measures. There are not even any voluntary federal standards.

(U) An additional component of the U.S. election infrastructure that requires immediate, mandatory cybersecurity measures are the election night reporting websites run by the states. The Committee heard testimony about a Russian attack on Ukraine's web page for announcing results. That attacked allowed the Russians to use misinformation that left Ukraine in chaos for days after the election. As the Committee's expert witness warned, "[w]e need to look at that playbook. They will do it to us."[11] Like voter registration databases, election results websites are not subject to any mandatory standards. Both of these critical vulnerabilities, as well as vulnerabilities of voting machines, must be addressed by the U.S. Congress through the passage of S. 2238, the Senate version of the SAFE Act.

(U) Given the inconsistent, and at times non-existent adherence to basic cybersecurity among states and localities, I cannot agree with the Committee's conclusion that "the country's decentralized election system can be a strength from a cybersecurity perspective." Until election security measures are required of every state and locality, there will be vulnerabilities to be exploited by our adversaries. The persistence of those vulnerabilities has national consequences. The manipulation of votes or voter registration databases in any county in the country can change the result of a national election. The security of the U.S. election system thus hinges on its weakest links – the least capable, least resourced local election offices in the country, many of which do not have a single full-time employee focused on cybersecurity.

(U) Every American has a direct stake in the cybersecurity of elections throughout the country. Congress has an obligation to protect the country's election system everywhere. If there were gaps in the defense of our coastline or air space, members would ensure that the federal government close them. Vulnerabilities in the country's election cybersecurity require the same level of national commitment.

(U) Cybersecurity vulnerabilities and influence campaigns

(U) The cybersecurity vulnerabilities of the U.S. election system cannot be separated from Russia's efforts to influence American voters. As the January 2017 Intelligence Community Assessment (ICA) concluded, and as the Committee report notes, the Russians were "prepared to publicly call into question the validity of the results" and "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory." This plan highlights an additional reason why nation-wide election cybersecurity standards are so critical. If Russia's preferred candidate does not prevail in the 2020 election, the

[10] Testimony of Alex J. Halderman, Professor of Computer Science and Engineering, University of Michigan, June 21, 2017.
[11] Testimony of Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs, Harvard Kennedy School, March 21, 2018.

Russians may seek to delegitimize the election. The absence of any successful cyber intrusions, exfiltrations or manipulations would greatly benefit the U.S. public in resisting such a campaign.

(U) While not formally part of the U.S. election infrastructure, the devices and accounts of candidates and political parties represent an alarming vulnerability in the country's overall election system. Russia's campaign of hacking the emails of prominent political figures and releasing them through Wikileaks, Gucifer 2.0, and DCLeaks was probably its most effective means of influencing the 2016 election. The Committee has received extensive testimony about these operations, the vulnerabilities that allowed them to occur, and the threat those vulnerabilities pose to the integrity of American democracy.[12] Yet little has been done to prevent it from happening all over again. S. 1569, the Federal Campaign Cybersecurity Assistance Act of 2019, addresses these vulnerabilities head on by authorizing political committees to provide cybersecurity assistance to candidates, campaigns and state parties.

(U) These vulnerabilities extend to the U.S. Senate, most of whose members are or will be candidates for reelection or for other positions. As a November 2018 Senate report noted, there is "mounting evidence that Senators are being targeted for hacking, which could include exposure of personal data."[13] Private communications and information reside on personal accounts and devices. Passage of S. 890, the Senate Cybersecurity Protection Act, will authorize the Senate Sergeant at Arms to protect the personal devices and accounts of Senators and their staff and help prevent the weaponization of their data in campaigns to influence elections.

(U) Assessments related to the 2016 election

(U) I have also submitted these Minority Views to address assessments related to Russian activities during the 2016 election. According to the January 2017 ICA, DHS assessed that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." An assessment based on observations is only as good as those observations and this assessment, in which DHS had only moderate confidence,[14] suffered from a lack of observable data. As Acting Deputy Undersecretary of Homeland Security for National Protection and Programs Directorate, Jeannette Manfra, testified at the Committee's June 21, 2017, hearing, DHS did not conduct any forensic analysis of voting machines.

(U) DHS's prepared testimony at that hearing included the statement that it is "likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected." The language of this assessment raises questions, however, about DHS's ability to identify cyber manipulation that could have affected a very close national election, particularly given DHS's acknowledgment of the "possibility that individual or isolated cyber

[12] See, for example, Committee hearing, March 30, 2017.
[13] Senators' Personal Cybersecurity Working Group Report, submitted by the Senators' Personal Cybersecurity Working Group, November 2018.
[14] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following Committee hearing, June 21, 2017.

intrusions into U.S. election infrastructure could go undetected, especially at local levels."[15] Moreover, DHS has acknowledged that its assessment with regard to the detection of outcome-changing cyber manipulation did not apply to state-wide or local elections.[16]

(U) Assessments about manipulations of voter registration databases are equally hampered by the absence of data. As the Committee acknowledges, it "has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases." Assessments about Russian attacks on the administration of elections are also complicated by newly public information about the infiltration of an election technology company. Moreover, as the Special Counsel reported, the GRU sent spear phishing emails to "Florida county officials responsible for administering the 2016 election" which "enabled the GRU to gain access to the network of at least one Florida county government."[17]

(U) The Committee, in stating that it had found no evidence that vote tallies were altered or that voter registry files were deleted or modified, rightly noted that the Committee's and the IC's insight into this aspect of the 2016 election was limited. I believe that the lack of relevant data precludes attributing any significant weight to the Committee's finding in this area.

(U) The Committee's investigation into other aspects of Russia's interference in the 2016 election will be included in subsequent chapters. I look forward to reviewing those chapters and hope that outstanding concerns about members' Committee staff access to investigative material, including non-compartmented and unclassified information, will be resolved.

---

[15] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[16] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[17] Report on the Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller III, March 2019

ADDITIONAL VIEWS OF SENATORS HARRIS, BENNET, AND HEINRICH

(U) The Russian government's attack on the 2016 election was the product of a deliberate, sustained, and sophisticated campaign to undermine American democracy. Russian military intelligence carried out a hacking operation targeting American political figures and institutions. The Internet Research Agency—an entity with ties to Russian President Vladimir Putin—used social media to sow disinformation and discord among the American electorate. And, as this report makes clear, individuals affiliated with the Russian government launched cyber operations that attempted to access our nation's election infrastructure, in some cases succeeding.

(U) The Russian objectives were clear: deepen distrust in our political leaders; exploit and widen divisions within American society; undermine confidence in the integrity of our elections; and, ultimately, weaken America's democratic institutions and damage our nation's standing in the world. The Committee did not discover evidence that Russia changed or manipulated vote tallies or voter registration information, however Russian operatives undoubtedly gained familiarity with our election systems and voter registration infrastructure—valuable intelligence that it may seek to exploit in the future.

(U) The Committee's report does not merely document the wide reach of the Russian operation; the report reveals vulnerabilities in our election infrastructure that we must collectively address. We do not endorse every recommendation in the Committee's report, and we share some of our colleagues' concerns about the vulnerability that we face, particularly at the state level, where counties with limited resources must defend themselves against sophisticated nation-state adversaries. Nevertheless, the report as a whole makes an important contribution to the public's understanding of how Russia interfered in 2016, and underscores the importance of working together to defend against the threat going forward.

(U) It is critical that state and local policymakers study the report's findings and work to secure election systems by prioritizing cybersecurity, replacing outdated systems and machines, and implementing audits to identify and limit risk. The Intelligence Community and other federal agencies must improve efforts to detect cyberattacks, enhance coordination with state and local officials, and develop strategies to mitigate threats. And, critically, Congress must take up and pass legislation to secure our elections. We must provide states the funding necessary to modernize and maintain election infrastructure, and we must take commonsense steps to safeguard the integrity of the vote, such as requiring paper ballots in all federal elections.

(U) Our adversaries will persist in their efforts to undermine our shared democratic values. In order to ensure that our democracy endures, it is imperative that we recognize the threat and make the investments necessary to withstand the next attack.

116TH CONGRESS *1st Session* | SENATE | REPORT 116-XX

(U) REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION

VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA

WITH ADDITIONAL VIEWS

[redacted]

CONTENTS

[redacted]

I. (U) INTRODUCTION

[redacted] In 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency (IRA) used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States.[1] [redacted] Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election. [redacted]

(U) The Senate Select Committee on Intelligence undertook a study of these events, consistent with its congressional mandate to oversee and conduct oversight of the intelligence activities and programs of the United States Government, to include the effectiveness of the Intelligence Community's counterintelligence function. In addition to the work of the professional staff of the Committee, the Committee's findings drew from the input of cybersecurity professionals, social media companies, U.S. law enforcement and intelligence agencies, and researchers and experts in social network analysis, political content, disinformation, hate speech, algorithms, and automation, working under the auspices of the Committee's Technical Advisory Group (TAG).[3] The efforts of these TAG researchers led to the release of two public reports on the IRA's information warfare campaign, based on data provided to the Committee by the social media companies.[4] These reports provided the

---

[1] **(U)** For purposes of this Volume, "information warfare" refers to Russia's strategy for the use and management of information to pursue a competitive advantage. *See* Congressional Research Service, *Defense Primer: Information Operations*, December 18, 2018.

[2] [redacted]

[3] **(U)** The TAG is an external group of experts the Committee consults for substantive technical advice on topics of importance to Committee activities and oversight. In this case, the Committee requested the assistance of two independent working groups, each with the technical capabilities and expertise required to analyze the data. The two working groups were led by three TAG members, with John Kelly, the founder and CEO of the social media analytics firm Graphika, and Phil Howard, an expert academic researcher at the Oxford Internet Institute, leading one working group, and Renee DiResta, the Director of Research at New Knowledge, a cybersecurity company dedicated to protecting the public sphere from disinformation attacks, leading the other.

[4] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/; Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018,

Committee, social media companies, U.S. law enforcement, international partners, fellow researchers and academics, and the American public with an enhanced understanding of how Russia-based actors, at the direction of the Russian government, effectuated a sustained campaign of information warfare against the United States aimed at influencing how this nation's citizens think about themselves, their government, and their fellow Americans. The Committee supports the findings therein.

(U) The Committee also engaged directly with a number of social media companies in the course of this study. The willingness of these companies to meet with Members and staff, share the results of internal investigations, and provide evidence of foreign influence activity collected from their platforms was indispensable to this study. Specifically, the Committee's ability to identify Russian activity on social media platforms was limited. As such, the Committee was largely reliant on social media companies to identify Russian activity and share that information with the Committee or with the broader public. Thus, while the Committee findings describe a substantial amount of Russian activity on social media platforms, the full scope of this activity remains unknown to the Committee, the social media companies, and the broader U.S. Government.

II. (U) FINDINGS

1. **(U)** The Committee found that the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin.

   (U) The Committee found that the IRA's information warfare campaign was broad in scope and entailed objectives beyond the result of the 2016 presidential election. Further, the Committee's analysis of the IRA's activities on social media supports the key judgments of the January 6, 2017 Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent US Elections," that "Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."[5] However, where the Intelligence Community assessed that the Russian government "aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him," the Committee found that IRA social media activity was overtly and almost invariably supportive of then-candidate Trump, and to the detriment of Secretary Clinton's campaign.[6]

---

https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[5] **(U)** Office of the Director of National Intelligence (ODNI), "Assessing Russian Activities and Intentions in Recent US Elections," *Intelligence Community Assessment (Unclassified Version),* January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[6] **(U)** *Ibid.*

(U) The Committee found that the Russian government tasked and supported the IRA's interference in the 2016 U.S. election. This finding is consistent with the Committee's understanding of the relationship between IRA owner Yevgeniy Prigozhin and the Kremlin, the aim and scope of the interference by the IRA, and the correlation between the IRA's actions and electoral interference by the Russian government in other contexts and by other means.[7] Despite Moscow's denials, the direction and financial involvement of Russian oligarch Yevgeniy Prigozhin, as well as his close ties to high-level Russian government officials including President Vladimir Putin, point to significant Kremlin support, authorization, and direction of the IRA's operations and goals.

[redacted]

2. **(U)** The Committee found that Russia's targeting of the 2016 U.S. presidential election was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society. Moreover, the IRA conducted a vastly more complex and strategic assault on the United States than was initially understood. The IRA's actions in 2016 represent only the latest installment in an increasingly brazen interference by the Kremlin on the citizens and democratic institutions of the United States.

[redacted] Russia's history of using social media as a lever for online influence operations predates the 2016 U.S. presidential election and involves more than the IRA. The IRA's operational planning for the 2016 election goes back at least to 2014, when two IRA operatives were sent to the United States to gather intelligence in furtherance of the IRA's objectives.[9] [redacted]

[7] **(U)** Indictment, *United States v. Internet Research Agency*, et al., Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[8] [redacted]

[9] **(U)** Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election – Unraveling the Russia Story So Far," *The New York Times,* September 20, 2018.

[10] [redacted]

[11] [redacted]

[12] **(U)** *Ibid.*

(U) Analysis of the behavior of the IRA-associated social media accounts makes clear that while the Russian information warfare campaign exploited the context of the election and election-related issues in 2016, the preponderance of the operational focus, as reflected repeatedly in content, account names, and audiences targeted, was on socially divisive issues—such as race, immigration, and Second Amendment rights—in an attempt to pit Americans against one another and against their government. The Committee found that IRA influence operatives consistently used hot-button, societal divisions in the United States as fodder for the content they published through social media in order to stoke anger, provoke outrage and protest, push Americans further away from one another, and foment distrust in government institutions. The divisive 2016 U.S. presidential election was just an additional feature of a much more expansive, target-rich landscape of potential ideological and societal sensitivities.

3. **(U)** The Committee found that the IRA targeted not only Hillary Clinton, but also Republican candidates during the presidential primaries. For example, Senators Ted Cruz and Marco Rubio were targeted and denigrated, as was Jeb Bush.[14] As Clint Watts, a former FBI Agent and expert in social media weaponization, testified to the Committee, "Russia's overt media outlets and covert trolls sought to sideline opponents on both sides of the political spectrum with adversarial views towards the Kremlin." IRA operators sought to impact primaries for both major parties and "may have helped sink the hopes of candidates more hostile to Russian interests long before the field narrowed."[15]

4. **(U)** The Committee found that no single group of Americans was targeted by IRA information operatives more than African-Americans. By far, race and related issues were the preferred target of the information warfare campaign designed to divide the country in 2016. Evidence of the IRA's overwhelming operational emphasis on race is evident in the IRA's Facebook advertisement content (over 66 percent contained a term related to race) and targeting (locational targeting was principally aimed at African-Americans in key metropolitan areas with), its Facebook pages (one of the IRA's top-performing pages, "Blacktivist," generated 11.2 million engagements with Facebook users), its Instagram content (five of the top 10 Instagram accounts were focused on African-American issues and audiences), its Twitter content (heavily focused on hot-button issues with racial undertones, such as the NFL kneeling protests), and its YouTube

[13] [redacted]

[14] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018); Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018.

[15] **(U)** Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

activity (96 percent of the IRA's YouTube content was targeted at racial issues and police brutality).

5. **(U)** The Committee found that paid advertisements were not key to the IRA's activity, and moreover, are not alone an accurate measure of the IRA's operational scope, scale, or objectives, despite this aspect of social media being a focus of early press reporting and public awareness.[16] An emphasis on the relatively small number of advertisements, and the cost of those advertisements, has detracted focus from the more prevalent use of original, free content via multiple social media platforms. According to Facebook, the IRA spent a total of about $100,000 over two years on advertisements—a minor amount, given the operational costs of the IRA were approximately $1.25 million dollars a month.[17] The nearly 3,400 Facebook and Instagram advertisements the IRA purchased are comparably minor in relation to the over 61,500 Facebook posts, 116,000 Instagram posts, and 10.4 million tweets that were the original creations of IRA influence operatives, disseminated under the guise of authentic user activity.

6. **(U)** The Committee found that the IRA coopted unwitting Americans to engage in offline activities in furtherance of their objectives. The IRA's online influence operations were not constrained to the unilateral dissemination of content in the virtual realm, and its operatives were not just focused on inciting anger and provoking division on the internet. Instead, the IRA also persuaded Americans to deepen their engagement with IRA operatives. For example, the IRA targeted African-Americans over social media and attempted and succeeded in some cases to influence their targets to sign petitions, share personal information, and teach self-defense training courses.[18] In addition, posing as U.S. political activists, the IRA requested—and in some cases obtained—assistance from the Trump Campaign in procuring materials for rallies and in promoting and organizing the rallies.[19]

7. **(U)** The Committee found that the IRA was not Russia's only vector for attempting to influence the United States through social media in 2016. Publicly available information showing additional influence operations emanating from Russia unrelated to IRA activity make clear the Kremlin was not reliant exclusively on the IRA in 2016. Russia's intelligence services, including the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), also exploited U.S. social media platforms as a

[16] **(U)** Dan Keating, Kevin Schaul and Leslie Shapiro, "The Facebook ads Russians targeted at different groups," *Washington Post,* November 1, 2017.
[17] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[18] **(U)** Shelby Holliday and Rob Barry, "Russian Influence Campaign Extracted Americans' Personal Data," *Wall Street Journal,* March 7, 2018.
[19] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

vehicle for influence operations.[20] Information acquired by the Committee from intelligence oversight, social media companies, the Special Counsel's investigative findings, and research by commercial cybersecurity companies all reflect the Russian government's use of the GRU to carry out another core vector of attack on the 2016 election: the dissemination of hacked materials.

8. **(U)** The Committee found that IRA activity on social media did not cease, but rather increased after Election Day 2016. The data reveal increases in IRA activity across multiple social media platforms, post-Election Day 2016: Instagram activity increased 238 percent, Facebook increased 59 percent, Twitter increased 52 percent, and YouTube citations went up by 84 percent.[21] As John Kelly noted: "After election day, the Russian government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election."[22]

   (U) Though all of the known IRA-related accounts from the Committee's data set were suspended or taken down in the fall of 2017, outside researchers continue to uncover additional IRA social media accounts dedicated to spreading malicious content. According to an October 2018 study of more than 6.6 million tweets linking to publishers of intentionally false news and conspiracy stories, in the months before the 2016 U.S. election, "more than 80% of the disinformation accounts in our election maps are still active . . . [and] continue to publish more than a million tweets in a typical day."[23]

III. (U) THE REACH OF SOCIAL MEDIA

(U) Social media and its widespread adoption have changed the nature and practice of human interaction for much of the world. During the 2016 election campaign season, approximately 128 million Facebook users in the United States alone generated nearly nine billion interactions related to the 2016 U.S. presidential election.[24] In just the last month of the campaign, more than 67 million Facebook users in the United States generated over 1.1 billion likes, posts, comments, and shares related to Donald Trump. Over 59 million Facebook users in the United States generated over 934 million likes, posts, comments and shares related to Hillary Clinton. On Election Day, 115.3 million Facebook users in the United States generated 716.3

[20] **(U)** Adam Entous, Elizabeth Dwoskin, and Craig Timberg, "Obama tried to give Zuckerberg a wake-up call over fake news on Facebook," *Washington Post,* September 24, 2017.
[21] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.
[22] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[23] **(U)** Matthew Hindman and Vlad Barash, "Disinformation, 'Fake News' and Influence Campaigns on Twitter," Knight Foundation, October 4, 2018, https://knightfoundation.org/articles/seven-ways-misinformation-spread-during-the-2016-election.
[24] **(U)** Dana Feldman, "Election Day Dominated Facebook With Over 716M Election-Related Interactions," *Forbes,* November 9, 2016.

million interactions related to the election and viewed election-related videos over 640 million times.[25]

(U) The Twitter platform also featured prominently across the arc of the 2016 campaign season. Americans sent roughly one billion tweets and retweets about the election between the first primary debates in August 2015 and Election Day 2016.[26] The U.S. Election Day 2016 was the most-Tweeted Election Day ever, with worldwide users generating more than 75 million election-related tweets.[27]

(U) Political campaigns, in the ambition of harvesting this connectivity and speaking "directly" with as many voters as possible, have adapted and attempted to exploit this new media environment. Total digital advertisement spending related to the 2016 election cycle on social media reached $1.4 billion—a 789 percent increase over 2012.[28]

(U) Social media has created new virtual venues for American participation in the national political discourse, and offered a new channel for direct democratic engagement with elected officials, media representatives, and fellow citizens around the world. However, the same system of attributes that empowers these tools and their users to positively increase civic engagement and constructive dialogue lends itself to exploitation, which frequently materializes as the dissemination of intentionally false, misleading, and deliberately polarizing content.[29]

(U) According to one November 2016 analysis, in the final three months leading up to Election Day, calculated by total number of shares, reactions, and comments, the top-performing intentionally false stories on Facebook actually outperformed the top news stories from the nineteen major news outlets.[30] That analysis found that in terms of user engagement, the top two intentionally false election stories on Facebook included articles alleging Pope Francis' endorsement of Donald Trump for President (960,000 shares, reactions, and comments), and WikiLeaks' confirmation of Hillary Clinton's sale of weapons to ISIS (789,000 shares, reactions, and comments).[31]

---

[25] **(U)** Ivana Kottasova, "Trump's Win Smashes Social Media Records," *CNN*, November 9, 2016.
[26] **(U)** Bridget Coyne, "How #Election2016 was Tweeted so far," *Twitter Blog*, November 7, 2016.
[27] **(U)** Twitter, "6.8 Million Viewers Watch Twitter Live Stream of BuzzFeed News' Election Night Special," November 10, 2016, https://www.prnewswire.com/news-releases/68-million-viewers-watch-twitter-live-stream-of-buzzfeed-news-election-night-special-300360415.html.
[28] **(U)** Kate Kaye, "Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast TV Down 20%, Cable and Digital Way Up," *AdAge,* January 3, 2017.
[29] **(U)** The term "fake news" is not a useful construct for understanding the complexity of influence operations on social media in today's online ecosystem. The term's definition has evolved since the 2016 election and today, has been, at times, misappropriated to fit certain political and social perspectives.
[30] **(U)** Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," *Buzzfeed*, November 16, 2016, ("During these critical months of the campaign, 20 top-performing false election stories from hoax sites and hyper-partisan blogs generated 8,7111,000 shares, reactions and comments on Facebook. . . . Within the same time period, the 20 best performing election stories from 19 major news websites generated a total of 7,367,000 shares, reactions and comments on Facebook.")
[31] **(U)** *Ibid.*

(U) A September 2017 Oxford Internet Institute study of Twitter users found that, "users got more misinformation, polarizing, and conspiratorial content than professionally produced news."[32] According to the study, in the "swing state" of Michigan, professionally produced news was, by proportion, "consistently smaller than the amount of extremist, sensationalist, conspiratorial, masked commentary, fake news and other forms of junk news," and the ratio was most disproportionate the day before the 2016 U.S. election.[33,34] A National Bureau of Economic Research paper from January 2017 assessed that intentionally false content accounted for 38 million shares on Facebook in the last 3 months leading up to the election, which translates into 760 million clicks—or "about three stories read per American adult."[35]

(U) In conducting a broader analysis of false information dissemination, in what was described as "the largest ever study of fake news," researchers at MIT tracked over 125,000 news stories on Twitter, which were shared by three million people over the course of 11 years.[36,37] The research found that, "Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news than for false news about terrorism, natural disasters, science, urban legends, or financial information." The study also determined that false news stories were 70 percent more likely to be retweeted than accurate news, and that true stories take about six times as long to reach 1,500 people on Twitter as false stories do. According to the lead researcher in the study, Soroush Vosoughi, "It seems pretty clear that false information outperforms true information."[38]

(U) The spread of intentionally false information on social media is often exacerbated by automated, or "bot" accounts. The 2016 U.S. election put on full display the impact that more sophisticated automation and the proliferation of bots have had on American political discourse. Researchers at the University of Southern California who evaluated nearly 20 million election-related tweets assessed that about one-fifth of the political discourse around the 2016 election on Twitter may have been automated and the result of bot activity. This research, however, does not make clear what country the bot activity originated from, or whether the activity was

---

[32] **(U)** Phil Howard, et al., "Social Media, News and Political Information during the U.S. Election: Was Polarizing Content Concentrated in Swing States," Oxford Internet Institute, Project on Computational Propaganda, September 29, 2017, https://arxiv.org/ftp/arxiv/papers/1802/1802.03573.pdf.

[33] **(U)** A swing state is a U.S. state in which Republican and Democratic candidates have similar levels of support and which is likely to play a key role in the outcome of presidential elections.

[34] **(U)** Philip Howard, Gillian Bolsover, et al., "Junk News and Bots During the U.S. Election: What Were Michigan Voters Sharing Over Twitter?" Oxford Internet Institute, Project on Computational Propaganda, March 26, 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/03/What-Were-Michigan-Voters-Sharing-Over-Twitter-v2.pdf.

[35] **(U)** Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 election," *Journal of Economic Perspectives,* Volume 31, Number 2, Spring 2017, 211-236, http://www.nber.org/papers/w23089.

[36] **(U)** Soroush Vosoughi, et al., "The spread of true and false news online," *Science*, Volume 359, Issue 6380, March 9, 2018, http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf.

[37] **(U)** Robinson Meyer, "The Grim Conclusions of the Largest Ever Study of Fake News," *The Atlantic*, March 8, 2018: https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/.

[38] **(U)** *Ibid.*

necessarily malicious in nature. These researchers also concluded that "bots [were] pervasively present and active in the online political discussion about the 2016 U.S. presidential election," adding that "the presence of social media bots can indeed negatively affect democratic political discussion rather than improving it."[39] Arriving at a similar conclusion, an Oxford Internet Institute study of 17 million tweets posted during the 2016 election found that bots "reached positions of measurable influence," and "did infiltrate the upper cores of influence and were thus in a position to significantly influence digital communications during the 2016 U.S. election."[40]

(U) In testimony to the Committee, social media researcher John Kelly suggested that automated accounts focused on fringe political positions are far more active than the voices of actual people holding politically centrist views: "In our estimate, today the automated accounts at the far left and far right extremes of the American political spectrum produce as many as 25 to 30 times the number of messages per day on average as genuine political accounts across the mainstream." In other words, "the extremes are screaming while the majority whispers."[41] Taken as a whole, the attributes of social media platforms render them vulnerable for foreign influence operations intent on sowing discord throughout American society.

IV. (U) RUSSIAN USE OF DISINFORMATION

(U) Russia's attack on the 2016 election was a calculated and brazen assault on the United States and its democratic institutions, but this was not the Kremlin's first foray into asymmetric warfare against America. Russian interference in 2016 represents the latest and most sophisticated example of Russia's effort to undermine the nation's democracy through targeted operations. As the January 6, 2017, Intelligence Community Assessment states, Moscow's provocations "demonstrated a significant escalation in directness, level of activity, and scope of effort." However, the activities only "represent the most recent expression of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order."[42]

(U) Russia's intelligence services have been focused for decades on conducting foreign influence campaigns, or "active measures," and disinformation.[43,44] The Russian intelligence services "pioneered dezinformatsiya [disinformation] in the early twentieth century," and by the mid-1960's, had significantly invested in disinformation and active measures.[45] According to

---

[39] **(U)** Alessandro Bessi and Emilio Ferrara, "Social Bots Distort the 2016 US Presidential Election Online Discussion," *First Monday*, Volume 21, Number 11, 7 November 7, 2016, https://ssrn.com/abstract=2982233.
[40] **(U)** Samuel Woolley and Douglas Guilbeault, "Computational Propaganda in the United States of America: Manufacturing Consensus Online," Oxford Internet Institute Computational Propaganda Research Project, May 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-USA.pdf.
[41] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[42] **(U)** ODNI, "Background to 'Assessing Russian Activities and Intentions in Recent U.S. Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[43] **(U)** "Active measures" is a Soviet-era term now called "measures of support" by the Russian government.
[44] **(U)** Disinformation is the intentional spread of false information to deceive.
[45] **(U)** *"Dezinformatsiya"* is a Russian word, defined in the 1952 Great Soviet Encyclopedia as the "dissemination (in the press, on the radio, etc.) of false reports intended to mislead public opinion."

testimony Roy Godson and Thomas Rid provided to the Committee, over 10,000 individual disinformation operations were carried out during the Cold War involving approximately 15,000 personnel at its peak.[46,47]

A. (U) Russian Active Measures

(U) For decades, Soviet active measures pushed conspiratorial and disinformation narratives about the United States around the world. The KGB authored and published false stories and forged letters concerning the Kennedy assassination, including accounts suggesting CIA involvement in the killing. Martin Luther King, Jr. was the target of manufactured KGB narratives, as was Ronald Reagan. Russian intelligence officers planted anti-Reagan articles in Denmark, France, and India during his unsuccessful 1976 bid for the Republican presidential nomination. A declassified U.S. State Department document from 1981 outlines a series of realized Russian active measures operations, including the spread of falsehoods concerning U.S. complicity in the 1979 seizure of the Grand Mosque of Mecca and responsibility for the 1981 death of Panamanian General Omar Torrijos, as well as an elaborate deception involving multiple forgeries and false stories designed to undermine the Camp David peace process and to exacerbate tensions between the United States and Egypt.[48] Among the most widely known and successful active measures operations conducted during the Cold War centered on a conspiracy that the AIDS virus was manufactured by the United States at a military facility at Fort Detrick in Maryland. This fictional account of the virus' origin received considerable news coverage, both in the United States and in over forty non-Cold War aligned countries around the world.[49]

(U) In a 1998 CNN interview, retired KGB Major General Oleg Kalugin described active measures as "the heart and soul of Soviet intelligence":

> *Not intelligence collection, but subversion; active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO; to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.*[50]

(U) While this history of discrediting the United States with spurious rumors and disinformation is well-chronicled, Russia has continued the practice today.

---

[46] **(U)** Thomas Rid, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[47] **(U)** Roy Godson, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[48] **(U)** Department of State, "Soviet Active Measures: Forgery, Disinformation, Political Operations," Special Report No. 88, October 1981, https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.

[49] **(U)** Christopher M. Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive & the Secret History of the KGB*, Basic Books, 1985, p. 244.

[50] **(U)** Oleg Kalugin, "Inside the KGB: An interview with retired KGB Maj. Gen. Oleg Kalugin," *CNN*, January 1998.

(U) As Sergey Tretyakov, the former SVR (the foreign intelligence service of the Russian Federation, and a successor organization to the KGB) "rezident," or station chief for Russian intelligence in New York, wrote in 2008, "Nothing has changed. . . . Russia is doing everything it can today to embarrass the U.S."[51]

B. (U) Russia's Military and Information Warfare

(U) While active measures have long been a tool of the Russian intelligence services, a shift toward developing and honing the tools of information warfare represents a more recent development for the Russian conventional military and larger national security establishment.

(U) The embrace of asymmetric information operations resulted from a number of factors, but chiefly from the Russian national security establishment's belief that these operations are effective. Pavel Zolotarev, a retired major general in the Russian Army, explained, "We had come to the conclusion . . . that manipulation in the information sphere is a very effective tool."[52] That conclusion was reinforced by the perception that these operations are extremely difficult to defend against, particularly with multinational military alliances like NATO, which is built to deter and if necessary defeat a traditional, conventional military threat. Information warfare, in addition, is an extremely low-cost alternative to conventional military conflict.

(U) A lack of alternatives also motivates Russia's reliance on asymmetric tactics. Russia's national security establishment may have had no choice but to increase its asymmetric capabilities given its inability to compete with the West on a more traditional, military hard power basis. Former National Intelligence Officer for Russia and Eurasia Eugene Rumer stated in 2017 testimony to the Committee that Russia's information warfare toolkit "performs the function of the equalizer that in the eyes of the Kremlin is intended to make up for Russia's weakness vis-à-vis the West."[53]

[redacted]

[51] **(U)** *See* Evan Osnos, David Remnick, and Joshua Yaffa, "Trump, Putin, and the new Cold War," *New Yorker*, March 6, 2017.
[52] **(U)** *Ibid.*
[53] **(U)** Eugene Rumer, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.
[54] [redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

C. (U) Russia's Weaponization of Social Media

(U) Portending what was to come in 2016, General Philip Breedlove assessed in his September 2014 remarks to the NATO Wales Summit that, regarding Ukraine, "Russia is waging

[55] **(U)** *Ibid.*
[56] **(U)** *Ibid.*

the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[57] Social media platforms enabled Russia's Ukraine campaign, and aided materially in the realization of its military's adoption of information warfare doctrine.

(U) Compared to more traditional methods for information warfare used in the Cold War, Watts described social media as providing Russia a "cheap, efficient, and highly effective access to foreign audiences with plausible deniability of their influence."[58]

(U) Russia's aptitude for weaponizing internet-based social media platforms against the United States resulted from Moscow's experience conducting online disinformation campaigns against its own citizens for over a decade. Russia's online disinformation efforts are rooted in the early and mid-2000s, when the Kremlin sought to suppress opposition in the face of rapidly expanding internet-based communications.[59]

(U) Studying the technology used by its political opponents, the Kremlin hijacked the capabilities and weaponized their use against Russia's own people. Russia perfected the use of these tools and methods of information warfare over time, paving the way for its decision to similarly target the citizens of other countries. Russia has also continued its domestic deployment of these tools.

- [redacted]
- [redacted]

D. (U) Russian Social Media Tactics

(U) The Kremlin has honed and refined its social media disinformation tactics over the last decade. Lessons learned through information warfare campaigns directed both internally

---

[57] **(U)** *See* John Vandiver, "SACEUR: Allies must prepare for Russia 'hybrid war,'" *Stars and Stripes*, September 4, 2014.

[58] **(U)** Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[59] **(U)** Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CNA Analysis and Solutions, Occasional Paper Series, March 2017.

[60] [redacted]

[61] **(U)** *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Special Counsel Robert S. Mueller, III, March 2019.

and at the populations of regional neighbors provided Moscow valuable insights into how information and social media could be most effectively used against the West.

(U) Although the tactics employed by Russia vary from one campaign to the next, there are several consistent themes in the Russian disinformation playbook.

(U) High Volume and Multiple Channels. Russian disinformation efforts tend to be wide-ranging in nature, in that they utilize any available vector for messaging, and when they broadcast their messaging, they do so at an unremitting and constant tempo. Christopher Paul and Miriam Matthews from the RAND Corporation describe the Russian propaganda effort as a "firehose of falsehood," because of its "incredibly large volumes," its "high numbers of channels and messages," and a "rapid, continuous, and repetitive" pace of activity. Russia disseminates the disinformation calculated to achieve its objectives across a wide variety of online vehicles: "text, video, audio, and still imagery propagated via the internet, social media, satellite television and traditional radio and television broadcasting."[62] One expert, Laura Rosenberger of the German Marshall Fund, told the Committee that "[t]he Russian government and its proxies have infiltrated and utilized nearly every social media and online information platform—including Instagram, Reddit, YouTube, Tumblr, 4chan, 9GAG, and Pinterest."[63]

(U) The desired effect behind the high volume and repetition of messaging is a flooding of the information zone that leaves the target audience overwhelmed. Academic research suggests that an individual is more likely to recall and internalize the *initial* information they are exposed to on a divisive topic. As RAND researchers have stated, "First impressions are very resilient."[64] Because first impressions are so durable and resistant to replacement, being first to introduce narrative-shaping content into the information ecosystem is rewarded in the disinformation context.

(U) Merging Overt and Covert Operations. The modern Russian disinformation playbook calls for illicitly obtaining information that has been hacked or stolen, and then weaponizing it by disseminating it into the public sphere. The most successful Russian operations blend covert hacking and dissemination operations, social media operations, and fake personas with more overt influence platforms like state-funded online media, including RT and Sputnik.

(U) According to FBI:

[redacted]

[62] **(U)** Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood,' Propaganda Model," *RAND Corporation,* 2016, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.
[63] **(U)** Laura Rosenberger, Written Testimony, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[64] **(U)** Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood,' Propaganda Model," *RAND Corporation,* 2016, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

[redacted]

(U) Another notable example of Russia using social media platforms and news media to advance disinformation objectives occurred in Germany in 2016. At the center of the operation was a report that falsely accused Arab migrants of sexually assaulting a Russian-German girl. The incident originates with Lisa, a 13-year-old girl from Berlin, who was reported missing by her parents after failing to show up for school. Initially claiming to have been attacked by men of Middle Eastern or North African appearance, Lisa eventually admitted to having fabricated the entire story. Despite Lisa's admission to the police that her story was made up, her original account of kidnapping and rape catapulted across social media. While German law enforcement officials formally debunked the initial report, Russian state-controlled news media, including Channel One and later RT, promoted the social media-inspired and ardently anti-migrant fervor among the Russian-German populations, in particular on YouTube.

(U) Far-right political parties, some of whom are supported by the Kremlin, reacted to these false stories by protesting in Berlin, protests which were covered by RT cameras. Sputnik then claimed there was a potential police cover-up, citing reporting of its own claim as its only evidence. A few days later, as protests spread, Russian Foreign Minister Lavrov publicly disputed that Lisa's 30-hour disappearance was voluntary. Germany, he said, was "covering up reality in a politically correct manner for the sake of domestic politics."[66] The office of Chancellor Merkel was forced to respond, and the episode added to the confusion and fear surrounding the politically roiling migrant crisis in Germany.

(U) Speed. Speed is critical to Russia's use of disinformation. Online, themes and narratives can be adapted and trained toward a target audience very quickly. This allows Russia

[65] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.
[66] **(U)** Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *The New York Times Magazine,* September 13, 2017.

to formulate and execute information operations with a velocity that far outpaces the responsivity of a formal decision-making loop in NATO, the United States, or any other western democracy. For example, within hours of the downing of Malaysian Airlines Flight 17 over Ukraine, Russian media had introduced a menu of conspiracy theories and false narratives to account for the plane's destruction, including an alleged assassination attempt against President Putin, a CIA plot, an onboard explosive, and the presence of a Ukrainian fighter jet in the area.[67,68] Dutch investigators with the Joint Investigation Team determined later the plane was shot down by a surface-to-air missile fired from a Russia-provided weapon system used in separatist-held territory in Ukraine.

(U) Use of Automated Accounts and Bots. The use of automated accounts on social media has allowed social media users to artificially amplify and increase the spread, or "virulence," of online content. Russia-backed operatives exploited this automated accounts feature and worked to develop and refine their own bot capabilities for spreading disinformation faster and further across the social media landscape. In January 2018, Twitter disclosed its security personnel assess that over 50,000 automated accounts linked to Russia were tweeting election-related content during the U.S. presidential campaign.[69]

(U) Russian actors are prolific users of automated accounts and bots. Phil Howard, citing the findings of a study done by the Oxford Internet Institute, concluded that Russian Twitter networks "are almost completely bounded by highly automated accounts, with a high degree of overall automation." His study assessed that "some 45 percent of Twitter activity in Russia is managed by highly automated accounts," and that Ukraine remains "the frontline of experimentation in computational propaganda with active campaigns of engagement" between Russian and Ukrainian botnets.[70] Early automation was fairly primitive and easier to detect and disrupt, but malicious bot activity has continued to grow in sophistication.

(U) Use of Paid Internet "Trolls." The act of "trolling" online has been a feature of the internet eco-system since the development of online chat rooms, blogs, internet forums, and other early communications platforms. An internet "troll" is a real person sitting behind a keyboard who posts inflammatory, aggressive, harassing, or misleading messages online in an attempt to provoke a response from other users of social media.[71] Kremlin-backed entities have spent years professionalizing a cadre of paid trolls, investing in large-scale, industrialized "troll

---

[67] **(U)** Joel Gunter and Olga Robinson, "Sergei Skripal and the Russian disinformation game," *BBC News,* September 9, 2018.

[68] **(U)** Margaret Hartmann, "Russia's 'Conspiracy Theory': MH17 Shot Down by Ukrainian Fighter Jet or Missile," *New York Magazine,* July 22, 2014.

[69] **(U)** Twitter Public Policy Blog, "Update on Twitter's review of the 2016 US election," January 19, 2018.

[70] **(U)** Samuel Woolley and Phil Howard, "Computational Propaganda Worldwide: Executive Summary," Computational Propaganda Research Project, Oxford Internet Institute, University of Oxford, November 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

[71] **(U)** The concept of a "troll" online is subjective and can encompass a range of differing motivations, tactics, and objectives. For the purposes of this paper, the Committee is focused on professional "trolls" who are paid to engage in dialogue online and provide commentary and content on various social media and news channels.

farms," in order to obscure Moscow's hand and advance the aims of Russia's information operations both domestically and abroad.

(U) While Russia's use of trolls has been more widely exposed in recent years, one of the first public exposures came through WikiLeaks in early 2012 and subsequent reporting by *The Guardian*. According to data and documents provided to WikiLeaks by a group operating under the moniker "Anonymous," the Kremlin-backed youth group Nashi was paying a network of bloggers and trolls to support President Putin and undermine his political opposition online. These Putin-supported commentators were paid to comment on articles, "dislike" anti-Putin YouTube videos, and support smear campaigns against opposition leaders.[72]

(U) In 2015, NATO's Strategic Communications Center of Excellence commissioned research on the use of trolling in hybrid warfare, publishing its conclusions in the spring of 2016. The study, which was largely focused on discussions surrounding the Ukraine-Russia conflict, outlined a variety of influence techniques employed by trolls online, including the aggressive use of offensive slurs and attacks; utilization of irony and sarcasm; peddling conspiracy theories; employing profile pictures of young, attractive men and women; diverting discourse to other problems; posting misleading information on information sources like *Wikipedia*; emphasizing social divisions; and presenting indigestible amounts of data without sources or verification.[73]

(U) In addition to the aggressive and persistent pushing of Kremlin-narrated themes and content, a principal objective of the Russian internet troll appears to be stifling the democratic debate entirely.

(U) As journalist Adrian Chen of *The New Yorker* reported, the objectives for Russia's troll army are primarily "to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[74] Leonid Volkov, a Russian politician and supporter of opposition leader Alexei Navalny, told Chen, "The point [of Russian disinformation] is to create the atmosphere of hate, to make it so stinky that normal people won't want to touch it." He stressed, "Russia's information war might be thought of as the biggest trolling operation in history, and its target is nothing less than the utility of the Internet as a democratic space."[75] Exemplifying the assertion, a 2015 analysis by the Finnish public broadcasting company concluded that many Finns elect to simply disengage from online discussions due to trolling, as "they did not see the use of fighting with masses of aggressive comments or threatening messages."[76]

---

[72] **(U)** Miriam Elder, "Hacked emails allege Russian youth group Nashi paying bloggers," *The Guardian*, February 7, 2012.

[73] **(U)** Sanda Svetoka, et al., "Social Media as a Tool of Hybrid Warfare," NATO Strategic Communications Centre of Excellence, May 2016, https://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

[74] **(U)** Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks." *The New Yorker,* July 27, 2016.

[75] **(U)** *Ibid.*

[76] **(U)** Sanda Svetoka, et al., "Social Media as a Tool of Hybrid Warfare," NATO Strategic Communications Centre of Excellence, May 2016, https://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

(U) Manipulating Real People and Events. Russian-backed trolls pushing disinformation have also sought to connect with and potentially coopt individuals to take action in the real world. From influencing unwitting Americans to retweet or spread propaganda, to convincing someone to host a real world protest, Russian disinformation agents employ online methods to attract and exploit a wide range of real people.

(U) In testifying to the Committee in 2017, Clint Watts outlined three different types of potential real-world targets for Russian influence operators.[77] A class of "useful idiots" refers to unwitting Americans who are exploited to further amplify Russian propaganda, unbeknownst to them; "fellow travelers" are individuals ideologically sympathetic to Russia's anti-western viewpoints who take action on their own accord; and "agent provocateurs" are individuals who are actively manipulated to commit illegal or clandestine acts on behalf of the Russian government. As Watts explains, "Some people are paid for. Some are coerced. Some are influenced. Some agree. Some don't know what they're doing. . . . Where they fall on that spectrum may not matter ultimately." What matters most, he argues, is the message they are carrying and whether its reach is growing.[78]

E. (U) Features of Russian Active Measures

(U) Although information warfare can target an opposing government, its officials, or its combat forces, Russian information warfare on social media is often aimed squarely at attacking a society and its relationship to its own democratic institutions.. Modern Russian active measures on social media exhibit several notable features.

(U) Attacking the Media. Information warfare, at its core, is a struggle over information and truth. A free and open press—a defining attribute of democratic society—is a principal strategic target for Russian disinformation. As Soviet-born author Peter Pomerantsev notes, "The Kremlin successfully erodes the integrity of investigative and political journalism, producing a lack of faith in traditional media." He concludes, "The aim of this new propaganda is not to convince or persuade, but to keep the viewer hooked and distracted, passive and paranoid, rather than agitated to action."[79]

(U) Jakub Kalensky, a former official with the European Union's rapid response team created to counter Russian disinformation, similarly argues, "It's not the purpose to persuade someone with one version of events. The goal for Russia is to achieve a state in which the

---

[77] **(U)** Clint Watts, Hearing before the Senate Armed Services Committee, April 27, 2017, available at https://www.fpri.org/wp-content/uploads/2017/04/Watts-Testimony-Senate-Armed-Services-email-distro-Final.pdf.
[78] **(U)** Denise Clifton, "A Murder Plot, a Twitter Mob and the Strange Unmasking of a Pro-Kremlin Troll," *Mother Jones,* June 5, 2018.
[79] **(U)** Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," *Institute of Modern Russia*, 2014, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

average media consumer says, 'There are too many versions of events, and I'll never know the truth.'"[80]

(U) Fluid Ideology. Because the Kremlin's information warfare objectives are not necessarily focused on any particular, objective truth, Russian disinformation is unconstrained by support for any specific political viewpoint and continually shifts to serve its own self-interest. Provided the information space is rendered confused and clouded, Russia's information operatives are unencumbered and can support any and all perspectives.

(U) An August 2018 report on information manipulation commissioned by the French government notes that the Kremlin "can simultaneously support far right and far left movements, so long as they are in competition with one another." As examples, the report cites the downing of Malaysian Airlines Flight 17, the chemical attacks in the Syrian town of Douma, and the poisoning of Sergei and Yulia Skripal in Salisbury, England, as instances in which Kremlin-backed disinformation amplified far-fetched and mutually exclusive conspiracy theories on both sides of the political spectrum.[81] This key characteristic distinguishes modern day Russian operations from former Soviet Union-era active measures campaigns. Speaking to the resultant operational flexibility, Pomerantsev describes the transition: "Unlike in the Cold War, when Soviets largely supported leftist groups, a fluid approach to ideology now allows the Kremlin to simultaneously back far-left and far-right movements, greens, anti-globalists, and financial elites. The aim is to exacerbate divides and create an echo chamber of Kremlin support."[82]

(U) In sum, the modern-day Russian information warfare campaign combines the advantages of social media information delivery and the operational freedom of being ideologically agnostic.

(U) Exploiting Existing Fissures. Successful Russian active measures attempt to exploit societal divisions that already exist, rather than attempt to create new ruptures. Alexander Sharavin, the head of a military research institute and a member of the Academy of Military Sciences in Moscow, provides an illustrative example in relation to the Queen's popular appeal in the England: "If you go to Great Britain, for example, and tell them the Queen is bad, nothing will happen, there will be no revolution, because the necessary conditions are absent—there is no existing background for this operation." As Thomas Rid noted in his 2017 testimony to the Committee, "The tried and tested way of active measures is to use an adversary's existing weaknesses against himself, to drive wedges into pre-existing cracks: the more polarized a

[80] **(U)** *See* Joby Warrick and Anton Troianovski, "Agents of doubt," *Washington Post*, December 10, 2018.
[81] **(U)** Jean-Baptiste Jeangene Vilmer, et al., "Information Manipulation: A Challenge for our Democracies," Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.
[82] **(U)** Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," *Institute of Modern Russia*, 2014, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

society, the more vulnerable it is."[83] Institutions and norms that define western liberal democracies—open and competitive elections, free flow of information, vibrant press freedoms, freedom of speech, and diverse societies—are conducive to exploitation by anti-Western propagandists.

(U) Indirect Objectives. As western governments grapple with addressing an internet operating environment that at present favors Russia, democratic institutions and constituencies must also weigh the potential indirect objectives of Russian active measures. As the August 2018 French disinformation report points out, the desired objectives of disinformation on a population can be two-fold. The direct objective, discussed earlier in this Volume, uses information manipulation to push the target audience in a preferred direction. The indirect objective entices overreach by the targeted country's government—in essence, baiting governments to respond in a heavy-handed or improper fashion that is irreconcilable with the nation's principles and civil liberties. The *indirect* objective, is, according to the French report, "not so much to convince a population of this or that story as to lead governments to take measures that are contrary to their democratic, liberal values, which, in turn, will provoke a reaction."[84]

(U) Similarly, even the fear of active measures being unleashed on a society risks societal damage, whether the foreign capability exists or not. Democratic governments and populations must balance the need for calling out and shining light on Russian activities with remaining realistic and sober about Moscow's actual capabilities and their effectiveness.

(U) The public needs to be made aware of the tactics being directed at them, but there also needs to be appreciation for the limitations of those tactics. As Massimo Calabresi reports in his 2017 *Time* article on Russia's social media war on America, "the fear of Russian influence operations can be more damaging than the operations themselves. Eager to appear more powerful than they are, the Russians would consider it a success if you questioned the truth of your news sources, knowing that Moscow might be lurking in your Facebook or Twitter feed."[85]

V. (U) THE INTERNET RESEARCH AGENCY

(U) The IRA is an entity headquartered in St. Petersburg, Russia, which since at least 2013 has undertaken a variety of Russian active measures campaigns at the behest of the Kremlin. The IRA has conducted virtual and physical influence operations in Russia, the United States, and dozens of other countries. The IRA conducted a multi-million dollar, coordinated

[83] **(U)** Thomas Rid, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[84] **(U)** Jean-Baptiste Jeangene Vilmer, et al., "Information Manipulation: A Challenge for our Democracies," Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

[85] **(U)** Massimo Calabresi, "Inside Russia's Social Media War on America," *Time*, May 18, 2017.

effort to influence the 2016 U.S. election as part of a broader information campaign to harm the United States and fracture its society.[86]

A. (U) Yevgeniy Prigozhin and the Kremlin

(U) The IRA is funded and directed by Yevgeniy Prigozhin, a Russia oligarch who works to conduct intelligence operations, military activities, and influence operations globally on behalf of the Kremlin. The IRA is one of several companies Prigozhin owns. He has also been linked to the financing and direction of the Wagner Group, a contract security organization that provides unofficial paramilitary support for Russian military operations.

[redacted]

(U) Prigozhin is a businessman and restauranteur who acquired the nickname "Putin's Chef," in part for the numerous catering contracts his company was awarded by the Russian government, including one for President Putin's 2012 inauguration. Prigozhin's companies have branched into areas including online propaganda, harassment of opposition leaders, and contracting a privatized military force to fight in Ukraine and Syria. *Fontanka*, a leading St. Petersburg news website, has also reported that Prigozhin's companies have secured oil revenues from Syrian oil fields in exchange for providing soldiers to protect those fields.[88]

[redacted]

[86] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[87] [redacted]

[88] **(U)** Neil MacFarquhar, "Meet Yevgeny Prigozhin, the Russian Oligarch Indicted in U.S. Election Interference," *New York Times*, February 16, 2018.

[89] [redacted]

(U) Prigozhin was publicly exposed as the main financial supporter of the IRA as early as 2014,[90] and his close relationship with Putin has been reported in numerous media sources, with the two appearing together in public photographs."[91]

(U) Prigozhin and companies he controlled, along with nine other employees, were indicted in the District of Columbia for a number of criminal violations, including acting as unregistered foreign agents inside the United States.[92] Further, Prigozhin and his companies have been targeted by the U.S. Department of Treasury with sanctions for "interfering with or undermining election processes and institutions," with specific respect to the 2016 U.S. presidential election.[93] Demonstrating that IRA operations were related to the broader scope of the Kremlin's objectives, these sanctions were announced alongside additional designations against the FSB and the Russian military intelligence organization, the GRU. Both entities were also designated for their online efforts to target the U.S. Government and undermine the election.

(U) Despite these public connections to the Russian government, President Putin denies any knowledge of Prigozhin's trolling operation. The Committee finds this denial to be false.

[redacted]

B. (U) IRA Operations

[redacted]

[90] **(U)** Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed*, June 2, 2014.
[91] **(U)** Neil MacFarquhar, "Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as Putin's Cook," New York Times, February 16, 2018.
[92] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[93] **(U)** Department of Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.
[94] [redacted]
[95] **(U)** *Ibid.*
[96] **(U)** *Ibid.*

[redacted]

[redacted]

(U) According to the Special Counsel's Office, the IRA was funded as part of a larger interference operation called "Project Lakhta," which was part of a global set of operations undertaken both within Russia and abroad. The monthly budget for Project Lakhta "exceeded 73 million Russian rubles (over 1,250,000 U.S. dollars), including approximately one million rubles in bonus payments."[103]

C. (U) The Role of the IRA Troll

(U) A 2015 article by Adrian Chen in *The New York Times Magazine* provides a detailed open source account of the IRA's operations. According to that article, in 2015 the IRA had an estimated 400 employees who worked 12-hour shifts, divided between numerous departments, filling nearly 40 rooms. The trolls would create content on nearly every social media network—including LiveJournal, VKontakte (a Russia-based social media platform modeled after Facebook), Facebook, Twitter, and Instagram. Managers responsible for overseeing the trolls would monitor the workplace by CCTV and were "obsessed with statistics" like page views,

---

[97] [redacted]

[98] **(U)** *Ibid.*

[99] **(U)** *Ibid.*

[100] [redacted]

[101] **(U)** *Ibid.*

[102] **(U)** *Ibid.*

[103] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

posts, clicks, and traffic. One IRA employee, Ludmila Savchuk, described work shifts during which she was required to meet a quota of five political posts, 10 nonpolitical posts, and 150 to 200 comments on other trolls' postings.[104]

> **(U)** *The first thing employees did upon arriving at their desks was to switch on an Internet proxy service, which hid their I.P. addresses from the places they posted; those digital addresses can sometimes be used to reveal the real identity of the poster. Savchuk would be given a list of the opinions she was responsible for promulgating that day. Workers received a constant stream of 'technical tasks' —point-by-point exegeses of the themes they were to address, all pegged to the latest news.*[105]

(U) Savchuk's description largely matches similar depictions outlined in a series of leaked documents from an unidentified Russian hacker organization in June 2014. The leaked documents, purported to be attached to internal emails from within the IRA, describe the responsibilities of the IRA teams. As reported by *BuzzFeed* at the time:

> *On an average working day, the Russians are to post on news articles 50 times. Each blogger is to maintain six Facebook accounts publishing at least three posts a day and discussing the news in groups at least twice a day. By the end of the first month, they are expected to have won 500 subscribers and get at least five posts on each item a day. On Twitter, the bloggers are expected to manage 10 accounts with up to 2,000 followers and tweet 50 times a day.*[106]

(U) As a member of the Special Projects department of the IRA, Savchuk was responsible for creating and maintaining believable, fake personas online that would eventually seed pro-Kremlin narratives into their otherwise normal-looking online activities. One former employee said: "We had to write 'ordinary posts,' about making cakes or music tracks we liked, but then every now and then throw in a political post about how the Kiev government is fascist, or that sort of thing." Instructions for those political posts would come to the bloggers every morning as "technical tasks," which would have a "news line, some information about it, and a 'conclusion' that the commenters should reach."[107] As described by Chen, "The point was to weave propaganda seamlessly into what appeared to be the nonpolitical musings of an everyday person."[108]

(U) According to two former employees who spoke to *The Guardian*, trolls were paid based on their capabilities and the expertise required to maintain their particular fake personas. One employee who signed a non-disclosure agreement was paid around 45,000 rubles a month (roughly $700), while others could make up to 65,000 rubles (roughly $1,000) monthly if they

---

[104] **(U)** Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015.
[105] **(U)** *Ibid.*
[106] **(U)** Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed*, June 2, 2014.
[107] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015.
[108] **(U)** Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015.

were able to join the most prestigious wing of the IRA, the English-language trolls. Penalties were instituted for employees who failed to reach their quota or were caught copying previous posts as opposed to creating new content. The trolls worked "round the clock to flood Russian internet forums, social networks and the comments sections of western publications with remarks praising the President, Vladimir Putin, and raging at the depravity and injustice of the west."[109]

(U) One former employee's description of his work at the IRA is notable:

> *I arrived there, and I immediately felt like a character in the book '1984' by George Orwell—a place where you have to write that white is black and black is white. Your first feeling, when you ended up there, was that you were in some kind of factory that turned lying, telling untruths, into an industrial assembly line. The volumes were colossal—there were huge numbers of people, 300 to 400, and they were all writing absolute untruths. It was like being in Orwell's world.*[110]

(U) The Special Counsel's Office description of the IRA's activities is consistent with much of the reporting derived from interviews of former employees. As an example, the IRA indictment alleges in detail how IRA employees, referred to as "specialists," were tasked with creating fake social media accounts that purported to be U.S. citizens engaged on social media:

> *The specialists were divided into day-shift and night-shift hours and instructed to make posts in accordance with the appropriate U.S. time zone. The [IRA] also circulated lists of U.S. holidays so that specialists could develop and post appropriate account activity. Specialists were instructed to write about topics germane to the United States such as U.S. foreign policy and U.S. economic issues. Specialists were directed to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements."*[111]

(U) The indictment indicates that IRA management made efforts to monitor and track the impact of its online efforts, through measurables such as comments, likes, reposts, changes in audience size, and other metrics.[112]

[redacted]

[109] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015.
[110] **(U)** Anton Troianovski, "A former Russian troll speaks: 'It was like being in Orwell's world,'" *Washington Post,* February 17, 2018.
[111] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[112] **(U)** *Ibid.*

[redacted]

D. (U) Troll Narratives

(U) The IRA's trolls monitored societal divisions and were poised to pounce when new events provoked societal discord. For example, a former IRA troll interviewed by the *Guardian* in 2015 described his focus on race-related issues: "When there were black people rioting in the U.S. we had to write that U.S. policy on the black community had failed, Obama's administration couldn't cope with the problem, the situation is getting tenser. The negroes are rising up."[115]

[redacted]

(U) Leaked IRA documents from 2014 reveal a sophisticated approach to the various social media platforms aimed at ensuring trolls could evade online monitors. IRA employees were taught how to comment on each of the different websites so as to avoid being blocked or removed. As an example, one author outlined how to write for the fringe site WorldNetDaily: "Direct offense of Americans as a race are not published ('Your nation is a nation of complete idiots') . . . nor are vulgar reactions to the political work of Barack Obama."[117]

---

[113] [redacted]

[114] **(U)** *Ibid.*

[115] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015.

[116] [redacted]

[117] **(U)** Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed*, June 2, 2014.

(U) Developing and applying a familiarity with the American political space was also a critical function of the IRA trolling operation. According to a former employee interviewed by the news outlet *Dozhd*, IRA personnel were required to study and monitor tens of thousands of comments in order to better understand the language and trends of internet users in the United States. The ex-troll indicated that they were taught to avoid crude and offensive language that would be off-putting to the typical online reader.[118] According to the former employee, the IRA office dedicated to inflaming sentiments in the United States was prohibited from promoting anything about Russia or President Putin—primarily because, in the IRA's assessment, Americans do not normally talk about Russia. "Our goal wasn't to turn the Americans toward Russia . . . . Our task was to set Americans against their own government: to provoke unrest and discontent, and to lower Obama's support ratings."[119] IRA employees were trained to understand and exploit the nuances of politically sensitive issues in America, including taxes, LGBT rights, and the Second Amendment. Once IRA employees better understood the political fault lines and how Americans naturally argued online, their job was to incite them further and try to "rock the boat."[120]

(U) More recent open source reporting has provided fresh insight into the inner workings and goals of the IRA operation. Marat Mindiyarov, a former IRA troll, outlined for the Washington Post in 2018 how important Facebook became to the IRA. Mindiyarov described how workers in the Facebook Department of the IRA were paid twice as much and included a younger, more pop culturally literate crowd. In order to graduate to the Facebook Department, these trolls had to take a test to prove their English language skills, their ability to comment on American political nuance, and to confirm they had the necessary opposition to the United States.[121]

VI. (U) IRA ACTIVITIES AGAINST THE UNITED STATES IN 2016

A. (U) Origins of IRA Activity in the United States

(U) The IRA's foray into influence operations targeting the 2016 election began with a 2014 intelligence-gathering mission to the United States undertaken by two female employees: Anna Bogacheva and Aleksandra Krylova.

(U) Bogacheva worked for the IRA from the spring of 2014 to the fall of 2016.[122] Krylova, who began her employment in St. Petersburg in the fall of 2013 at the latest, rose to

---

[118] **(U)** Meduza, "An ex-St. Petersburg 'troll' speaks out," October 15, 2017 (summarizing an interview with "Maxim" by *Dozhd*).
[119] **(U)** *Ibid.*
[120] **(U)** *Ibid.*
[121] **(U)** Anton Troianovski, "A former Russian troll speaks: 'It was like being in Orwell's world,'" *Washington Post,* February 17, 2018.
[122] **(U)** Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election – Unraveling the Russia Story So Far," *The New York Times,* September 20, 2018: https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html?rref=collection%2Fsectioncollection%2Fpolitics.

become the IRA's third-highest ranking employee by the spring of 2014. Both secured visas to visit the United States in June 2014, and the two made stops in "Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York," according to the IRA indictment.[123]

[redacted] Operating as a reconnaissance team for the IRA, the two were sent to collect intelligence to be used in the organization's information warfare against the United States. Prior to the trip, they had worked with their colleagues to plan itineraries and purchase equipment, including "cameras, SIM cards, and drop phones." They also worked on various "evacuation scenarios" and other security measures for their trip.[124] Their visit likely helped the IRA refine tactics to be used on social media, but the trip represents only a small part of the wider operational effort to track and study Americans' online activities, understand U.S. political and social divisions, impersonate U.S. citizens online, and ultimately engage in information warfare against the United States. [redacted]

(U) According to the Special Counsel's Office, by April 2014, the IRA had formed a new department inside the larger organization that was focused solely on the U.S. population. Referred to as the "translator project," and alternately as the "Translator Department," the American department of the operation would grow to over 80 employees by July 2016.[126] By the summer of 2016, at the height of the U.S. campaign season, the "translator project" employees were posting more than 1,000 pieces of content per week, reaching between 20 and 30 million people in the month of September alone.[127] In addition, the IRA employees began contacting unwitting U.S. persons to better refine their tactics and targets. In one communication, an IRA operative posed as an American and spoke with a Texas-based grassroots organization, learning from the conversation that they should focus their activities on "purple states like Colorado, Virginia & Florida."[128]

---

[123] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[124] **(U)** *Ibid.*

[125] [redacted]

[126] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018); Special Counsel Robert S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, March 2019, Volume I, p. 26.

[127] **(U)** *See* Hannah Levintova, "Russian Journalists Just Published a Bombshell Investigation About a Kremlin-Linked 'Troll Factory,'" *Mother Jones*, October 18, 2017. Original report in Russian available at https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1.

[128] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[129] [redacted]

[130] **(U)** *Ibid.*

[131] [redacted]

[132] **(U)** *Ibid.*

(U) The IRA built a wide-ranging information operation designed to complement these other Russian influence activities directed toward interfering with and undermining U.S. democracy in 2016. The expanse and depth of this effort would only be understood in the aftermath of that campaign.

B. (U) IRA Operations Explicitly Targeting the 2016 U.S. Election

(U) At the direction of the Kremlin, the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump.[133]

(U) The overwhelming majority of the content disseminated by the IRA did not express clear support for one presidential candidate or another. Instead, and often within the context of the election or in reference to a candidate, most IRA content discreetly messaged narratives of disunity, discontent, hopelessness, and contempt of others, all aimed at sowing societal division. Nevertheless, a significant body of IRA content dealt with the election, and specifically the Republican and Democrat candidates. The TAG study led by Renee DiResta concluded that for all data analyzed, which included data captured before and after the 2016 U.S. election, roughly 6 percent of tweets, 18 percent of Instagram posts, and 7 percent of Facebook posts from IRA accounts mentioned Donald Trump or Hillary Clinton by name. On Facebook, that percentage translated to 1,777 posts that specifically mention Hillary Clinton (or a derivative moniker), which in turn generated over 1.7 million user interactions or engagements.[134]

(U) Numbers of posts are an imperfect and potentially misleading evidentiary base for drawing conclusions about motivations and objectives. The relatively low number of IRA Facebook and Twitter account posts that specifically mention either candidate is not dispositive of the IRA's intent to influence voters. In practice, the IRA's influence operatives dedicated the balance of their effort to establishing the credibility of their online personas, such as by posting innocuous content designed to appeal to like-minded users. This innocuous content allowed IRA influence operatives to build character details for their fake personas, such as a conservative Southerner or a liberal activist, until the opportune moment arrived when the account was used to deliver tailored "payload content" designed to influence the targeted user. By this concept of operations, the volume and content of posts can obscure the actual objective behind the influence operation. "If you're running a propaganda outfit, most of what you publish is factual so that

---

[133] **(U)** ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment (Declassified Version), January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.; Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller, III, March 2019.

[134] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

you're taken seriously," Graphika CEO and TAG researcher John Kelly described to the Commttee, "[T]hen you can slip in the wrong thing at exactly the right time."[135]

(U) The tactic of using select payload messages among a large volume of innocuous content to attract and cultivate an online following is reflected in the posts made to the IRA's "Army of Jesus" Facebook page. The page, which had attracted over 216,000 followers by the time it was taken down by Facebook for violating the platform's terms of service, purported to be devoted to Christian themes and Bible passages. The page's content was largely consistent with this façade. The following series of posts from the "Army of Jesus" page illustrates the use of this tactic, with the majority of posts largely consistent with the page's theme, excepting the November 1, 2016 post that represents the IRA's payload content:

- October 26, 2016: "There has never been a day when people did not need to walk with Jesus."
- October 29, 2016: "I've got Jesus in my soul. It's the only way I know. . . . Watching every move I make, guiding every step I take!"
- October 31, 2016: "Rise and shine—realize His blessing!"
- October 31, 2016: "Jesus will always be by your side. Just reach out to Him and you'll see!"
- November 1, 2016: "HILLARY APPROVES REMOVAL OF GOD FROM THE PLEDGE OF ALLEGIANCE."
- November 2, 2016: "Never hold on anything [sic] tighter than you holding unto God!"

(U) This pattern of character development, followed by confidence building and audience cultivation, punctuated by deployment of payload content is discernable throughout the IRA's content history.

(U) The IRA's ideologically left-leaning and right-leaning social media accounts posted content that was political in nature and made reference to specific candidates for President. Hillary Clinton, however, was the only candidate for President whose IRA-posted content references were uniformly negative. Clinton's candidacy was targeted by both the IRA's left and right personas, and both ideological representations were focused on denigrating her. As Renee DiResta notes, the political content of the IRA, "was unified on both sides in negativity towards Secretary Clinton."[136] The IRA's left-leaning accounts focused their efforts on denigrating

[135] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[136] **(U)** Renee DiResta, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

Clinton and supporting the candidacy of either fellow Democrat candidate Bernie Sanders or Green Party candidate Jill Stein, at the expense of Hillary Clinton. Posts from the IRA's right-leaning accounts were unvaryingly opposed to Clinton's candidacy.

(U) In contrast to the consistent denigration of Hillary Clinton, Donald Trump's candidacy received mostly positive attention from the IRA's influence operatives, though it is important to note that this assessment specifically applies to pre-election content. The Committee's analysis indicates that post-election IRA activity shifted to emphasize and provoke anti-Trump sentiment on the left. DiResta's team assesses that in relation to pre-election content: "The majority of the political content was anti-Hillary Clinton; there appeared to be a consistent preference for then-candidate Donald Trump, beginning in the early primaries. . . . There was no pro-Clinton content."[137]

(U) Evidence of an overarching pro-Trump and anti-Clinton bias leading up to Election Day 2016 is also found in information obtained by Special Counsel's Office. For instance, IRA employees were directed to focus on U.S. politics and to "use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them)."[138] Another IRA employee was criticized internally for having a "'low number of posts dedicated to criticizing Hillary Clinton' and was told 'it is imperative to intensify criticizing Hillary Clinton' in future posts."[139] Content and hashtags produced by IRA employees included "#Trump2016," "#TrumpTrain," "#MAGA," "#IWontProtectHillary," and "#Hillary4Prison."[140]

(U) One communication obtained by the Committee details an IRA employee's description of Election Day 2016, from the vantage of an information warfare operative: "On November 9, 2016, a sleepless night was ahead of us. And when around 8 a.m. the most important result of our work arrived, we uncorked a tiny bottle of champagne . . . took one gulp each and looked into each other's eyes. . . . We uttered almost in unison: 'We made America great.'"[141]

(U) Further, the IRA's attempts to engage political activists by using false U.S. personas to "communicate with unwitting members, volunteers, and supporters of the Trump Campaign involved in local community outreach, as well as grassroots groups that supported then-candidate Trump."[142]

---

[137] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.
[138] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[139] **(U)** *Ibid.*
[140] **(U)** *Ibid.*
[141] [redacted]
[142] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

(U) In addition to denigrating Hillary Clinton, voter suppression among left-leaning audiences appears to have been another political goal of the IRA's influence operatives. Young Mie Kim, a digital advertisement research expert from the University of Wisconsin, has closely analyzed the IRA's Facebook advertisements. On the basis of Kim's analysis, three types of voter suppression campaigns on Facebook and Instagram emerge, including: "a) turnout suppression/election boycott; b) third-candidate promotion; and c) candidate attack, all targeting nonwhites or likely Clinton voters."[143] Kim found no evidence of a comparable voter suppression effort that targeted U.S. voters on the ideological right.

(U) Renee DiResta found similar evidence:

> *Voter suppression narratives were in [the data], both on Twitter (some of the text-to-vote content) and within Facebook, where it was specifically targeting the Black audiences. So the groups that they made to reach out to Black people were specifically targeted with 'Don't Vote for Hillary Clinton,' 'Don't Vote At All,' 'Why Would We Be Voting,' 'Our Votes Don't Matter,' [and] 'A Vote for Jill Stein is Not a Wasted Vote.'*[144]

(U) TAG researcher Phil Howard's findings support DiResta's assessment. Howard found that while both the ideological right and left in America were targeted:

> *The main difference is that where Conservative and right-wing voters were actively encouraged to get behind Trump's campaign, other voters were encouraged to boycott the election, vote for someone other than Clinton, and become cynical of the political process in general.*[145]

(U) Underscoring the insidiousness of the IRA's information warfare campaign, influence operations were conducted in cognizance of the U.S. political schedule and political events. Modifying their tactics and strategy to reflect real-life occurrences, the IRA's operatives would increase their activity around events relevant to the campaign schedule. This included pre-election events, like "candidate debates, [the] Republican convention, [and] Trump crossing the delegate threshold."[146] For example, "significant bursts of IRA activity" coincided with the third Democratic primary debate in January 2016, the sixth Republican primary debate in January 2016, the presidential debates between Clinton and Trump in the fall of 2016, and on

---

[143] **(U)** Young Mie Kim, "Uncover: Strategies and Tactics of Russian Interference in US Elections," Project DATA, University of Wisconsin, Madison, September 4, 2018, https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/09/Uncover.Kim_.v.5.0905181.pdf.

[144] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[145] **(U)** Phil Howard, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[146] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

Election Day 2016.[147] More broadly, the volume of posts originating from IRA accounts on Facebook and Instagram increased over the period between the national political conventions in July 2016 and Election Day.[148]

(U) The IRA's information warfare campaign also responded to real-world political events. For example, the IRA promoted multiple stories and narratives calling into question the state of Hillary Clinton's health after she fell ill at a September 11 memorial service in New York City in September 2016. IRA influence operatives posted phrased content on Twitter using hashtags that made the content easily discoverable to other Twitter users searching for content related to Clinton's health, including #HillarySickAtGroundZero, #ClintonCollapse, #ZombieHillary, and #SickHillary. According to researchers at Clemson University, IRA accounts tweeted these hashtags hundreds of times. As one of those researchers, Darren Linvill, points out:

> *You can see the peak times they tweet. You can see that they shift from hour to hour. One hour, they'll tweet their left-wing accounts, and the next hour they'll tweet their right-wing accounts. . . . You can see very clearly that it is one organization, and it has applied human capital as is needed, depending on what's happening politically, what current events are.*[149]

[redacted] A particular spike in IRA activity on October 6, 2016, stands out as an anomaly deserving further scrutiny. As reported by the *Washington Post* and noted by the Clemson research team, IRA influence operatives posted, at a pace of about a dozen tweets per minute, nearly 18,000 messages from their Twitter accounts on October 6, 2016. This spike in activity came a day prior to WikiLeaks's publication of emails stolen by the Russian GRU from the account of Hillary Clinton's campaign chairman, John Podesta. According to the researchers, on October 6 and 7, IRA Twitter accounts—particularly those accounts emulating ideologically left-leaning personas—significantly increased the volume of their content posting, with 93 of the "Left Troll" accounts posting content that could have directly reached other Twitter accounts 20 million times on those two days.[150] While no clear connection between the spike in IRA Twitter activity and WikiLeaks' release of the emails has been established, the Clemson researchers speculate that the timing was not coincidental: "We think that they [the IRA] were trying to activate and energize the left wing of the Democratic Party, the Bernie wing basically, before the WikiLeaks release that implicated Hillary in stealing the Democratic primary."[151] [redacted]

---

[147] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[148] **(U)** *Ibid.*

[149] **(U)** Jim Galloway, "Clemson researchers crack open a Russian troll factory," *Associated Press,* August 7, 2018.

[150] **(U)** Craig Timberg and Shane Harris, "Russian operatives blasted 18,000 tweets ahead of a huge news day during the 2016 presidential campaign. Did they know what was coming?" *Washington Post*, July 20, 2018.

[151] **(U)** *Ibid.*

[redacted]

(U) As detailed by the Special Counsel's Office, IRA operations to support Trump also involved activities inside the United States. For example, IRA operatives were able to organize and execute a series of coordinated political rallies titled, "Florida Goes Trump," using the Facebook group "Being Patriotic," the Twitter account @March_for_Trump, and other fabricated social media personas. Masquerading as Americans, IRA operatives communicated with Trump Campaign staff, purchased advertisements promoting these rallies on Facebook and Instagram, contacted grassroots supporters of then-candidate Trump, solicited U.S. citizens to participate in these events, and even paid select participants to portray Hillary Clinton imprisoned in a cage that had been constructed on a flatbed truck for this purpose.[153]

C. (U) Other IRA Operations Targeting U.S. Politicians and Society

(U) The IRA targeted not only Hillary Clinton, but also Republican candidates during the presidential primaries. For example, Senators Ted Cruz and Marco Rubio were targeted and denigrated, as was Jeb Bush.[154] Even after the 2016 election, Mitt Romney—historically critical of Russia and who memorably characterized the country as the United States' "number one geopolitical foe" during a 2012 presidential debate—was targeted by IRA influence operatives while being considered for Secretary of State in the Trump administration. Content posted from IRA social media pages and accounts referred to Romney as a "two headed snake" and a "globalist puppet," and IRA operatives posted the hashtag "#NeverRomney," in an effort to undermine his potential nomination.[155] On November 28, 2016, over 216,000 followers of the IRA's "Being Patriotic" Facebook page received the following post in their News Feed: "Romney was one of the first men who started the NeverTrump movement. It will be a terrible mistake if Trump sets him as the next secretary of state."

(U) In addition, the IRA "had a strategic goal to sow discord in the U.S. political system," which included—but was not limited to—targeting the 2016 U.S. presidential election.[156] John Kelly found that "[i]t's a far more sophisticated an attack than just caring about an election. And it's not just one election they care about. They care about the electoral system."[157] Darren Linvill echoed this point, concluding "[I]n general, there's been too much

---

[152] [redacted]

[153] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[154] **(U)** *Ibid*; Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018: https://www.newknowledge.com/articles/the-disinformation-report/.

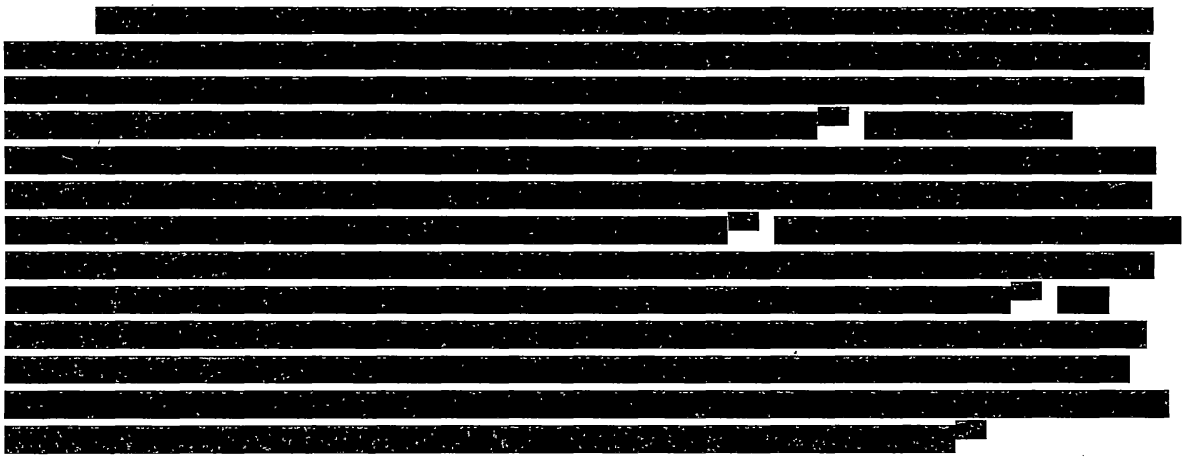
[155] **(U)** Rob Barry and Shelby Holliday, "Russian Trolls Tried to Torpedo Mitt Romney's Shot at Secretary of State," *Wall Street Journal*, March 8, 2018.

[156] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[157] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

focus on Russian interference in the election. It's much more than that. It's interference in our society, in our culture, in our political conversation."[158]

[redacted]



(U) No single group of Americans was targeted by IRA information operatives more than African-Americans. By far, race and related issues were the preferred target of the information warfare campaign designed to divide the country in 2016. Evidence of the IRA's overwhelming operational emphasis on race is evident in the IRA's Facebook advertisement content (over 66 percent contained a term related to race) and targeting (locational targeting was principally aimed at "African-Americans in key metropolitan areas with well-established black communities and flashpoints in the Black Lives Matter movement"), as well as its Facebook pages (one of the IRA's top-performing pages, "Blacktivist," generated 11.2 million engagements with Facebook users), its Instagram content (five of the top 10 Instagram accounts were focused on African-American issues and audiences), its Twitter content (heavily focused on hot-button issues with racial undertones such as the NFL kneeling protests), and its YouTube

[158] **(U)** Jim Galloway, "Clemson researchers crack open a Russian troll factory," *Associated Press,* August 7, 2018.
[159] [redacted]
[160] **(U)** *Ibid.*
[161] **(U)** *Ibid.*
[162] **(U)** *Ibid.*
[163] **(U)** *Ibid.*

activity (96 percent of the IRA's YouTube content was targeted at racial issues and police brutality).

(U) The IRA's exploitation of racial tensions in an attempt to sow societal discord in the United States is not a new tactic for Russian influence operations. Rather, it is the latest incarnation of a long-standing Russian focus. Historically, the KGB's active measures program also made race a central feature of its operational targeting. As KGB archivist Vasili Mitrokhin noted: "The attempt to stir up racial tensions in the United States remained part of Service A's stock-in-trade for the remainder of the Cold War." For example, before the Los Angeles Olympics in 1984, KGB officers mailed falsified communications from the Ku Klux Klan to the Olympic committees of African and Asian countries. KGB officers also forged letters that were "sent to sixty black organizations giving fictitious details of atrocities committed by the [Jewish Defense] League against blacks."[164]

(U) As the TAG study led by Renee DiResta concluded:

> *The most prolific IRA efforts on Facebook and Instagram specifically targeted Black American communities and appear to have been focused on developing Black audiences and recruiting Black Americans as assets. . . . While other distinct ethnic and religious groups were the focus of one or two Facebook Pages or Instagram accounts, the Black community was targeted extensively with dozens; this is why we have elected to assess the messaging directed at Black Americans as a distinct and significant operation.*[165]

(U) In March 2018, the *Wall Street Journal* was among the first to report on a series of elaborate efforts by IRA operatives to target, coopt, and incite African-Americans to participate in real world activities the IRA promoted online. African-Americans targeted on social media were asked to deepen their engagement with IRA operatives—from signing petitions to teaching self-defense training courses. In one instance cited by the *Wall Street Journal*, operatives used the IRA Facebook page, "Black4Black," to solicit from African-American-led businesses in Cleveland, Ohio personal information in exchange for free promotions on social media.[166] IRA operatives also spearheaded and funded a self-defense program that entailed African-American trainers being paid to teach courses in their communities. As part of this operation, an African-American activist was paid roughly $700 to teach 12 self-defense classes in a local park under the auspices of the IRA-administered "BlackFist" Facebook page.[167]

---

[164] **(U)** Christopher M. Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive & the Secret History of the KGB*, Basic Books, 1985, p. 244.

[165] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[166] **(U)** Shelby Holliday and Rob Barry, "Russian Influence Campaign Extracted Americans' Personal Data," *Wall Street Journal,* March 7, 2018.

[167] **(U)** *Ibid.*

(U) Although the specific objectives behind the IRA's efforts to animate American social media users to organize around political and cultural identification is not entirely evident from the available data, the general intent to foment and promote divisiveness and discord amongst the American populace is strongly evidenced, as are the desire and capability of the IRA to effectively coopt unwitting Americans.

D. (U) IRA Use of Paid Advertisements

(U) Paid advertisements were not key to the IRA's activity, and moreover, are not alone an accurate measure of the IRA's operational scope, scale, or objectives, despite this aspect of social media being a focus of early press reporting and public awareness. According to Facebook, the IRA spent a total of about $100,000 over two years on advertisements—a minor amount, given the operational costs of the IRA are estimated to have been around $1.25 million dollars a month. The nearly 3,400 Facebook and Instagram advertisements the IRA purchased are comparably minor in relation to the over 61,500 Facebook posts, 116,000 Instagram posts, and 10.4 million tweets that were the original creations of IRA influence operatives, disseminated under the guise of authentic user activity. Further, numerous high-profile U.S. persons, such as Roger Stone, Michael McFaul, and Sean Hannity, unwittingly spread IRA content by liking IRA tweets or engaging with other IRA social media content, enhancing the potential audience for IRA content by millions of Americans.

(U) An analysis of the audiences targeted for receipt of those advertisements on Facebook nonetheless indicates that the IRA's use of advertising was consistent with its overall approach to social media. In particular, the IRA targeted some election swing states with advertisements that leveraged socially incendiary and divisive subjects. According to the report produced by the TAG working group led by Phil Howard and John Kelly, Facebook users in swing states were targeted 543 times, out of 1,673 instances of location targeting by the IRA. Additionally, in 342 instances, areas with significant African-American populations were targeted by the IRA with Facebook advertisements. TAG researchers believe that the targeting had more to do with race than a state's role in the Electoral College or status as a swing state:

> *We found from the data that location targeting of ads was not used extensively by the IRA, with only 1,673 different instances of location targeting, by 760 ads. These ads were usually used to target African Americans in key metropolitan areas with well-established black communities and flashpoints in the Black Lives Matter movement. Some make reference, for example, to Ferguson, MO, and a smaller group of ads that marketed rallies and demonstrations to users living in particular places.*[168]

---

[168] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018: https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

(U) The parameters and key terms the IRA employed in targeting its Facebook advertisements suggests a sophisticated understanding of where the rawest social sensitivities lie beneath the surface of the American political debate. Darren Linvill noted that the IRA had a "keen understanding of American psychology," they knew "exactly what buttons to press," and operated with "industrial efficiency."[169] Even so, the IRA failed to take advantage of more sophisticated targeting capabilities available to Facebook advertising customers. For example, IRA operatives did not utilize the "Custom Audiences" feature which would have allowed them to upload outside data and contact information, and permitted more advanced micro-targeting of their advertisements.[170]

[redacted]

E. (U) The IRA Information Warfare Campaign

[redacted]

[169] **(U)** Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election – Unraveling the Russia Story So Far," *New York Times,* September 20, 2018.

[170] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf ("The targeting for the IRA ads that we have identified and provided to the Committee was relatively rudimentary, targeting broad locations and interests, and did not use a tool known as Contact List Custom Audiences.")

[171] [redacted]

[172] **(U)** *Ibid.*

[173] [redacted]

(U) Disinformation experts agree with Prigozhin's assessment. Clint Watts, in March 2017 testimony to the Committee: "Over the past three years, Russia has implemented and run the most effective and efficient influence campaign in world history."[174]

(U) Eugene Rumer elaborated on Watts' point in offering this summary in March 2017 testimony to the Committee:

> *Russian meddling in the 2016 U.S. Presidential election is likely to be seen by the Kremlin as a major success regardless of whether its initial goal was to help advance the Trump candidacy. The payoff includes, but is not limited to a major political disruption in the United States, which has been distracted from many strategic pursuits; the standing of the United States and its leadership in the world have been damaged; it has become a common theme in the narrative of many leading commentators that from the pillar of stability of the international liberal order the United States has been transformed into its biggest source of instability; U.S. commitments to key allies in Europe and Asia have been questioned on both sides of the Atlantic and the Pacific. And last, but not least, the Kremlin has demonstrated what it can do to the world's sole remaining global superpower.*[175]

(U) Thomas Rid echoed this conclusion before the Committee: "The great Active Measures campaign of 2016 will be studied in intelligence schools for decades to come, not just in Russia of course but in other countries as well."[176]

F. (U) Ongoing IRA Activities

(U) IRA activity on social media did not cease, but rather increased after Election Day 2016. Evidence from well-known IRA accounts confirms that Russia-based operatives continued to be actively exploiting divisive social issues in the United States well after the 2016 election. After Election Day, Left-leaning IRA accounts were promoting hashtags such as "#Impeach45," "#Resist," and "#GunReformNow." Complementary right-leaning IRA accounts were focused on the NFL kneeling controversy, as well as hashtags critical of the FBI, such as the "#ReleaseTheMemo" meme. After the election, IRA operatives orchestrated disparate political rallies in the United States both supporting president-elect Trump, and protesting the results of the election. A mid-November 2016 rally in New York was organized around the theme, "show your support for President-Elect Donald Trump," while a separate rally titled, "Trump is NOT my President," was also held in New York, in roughly the same timeframe.[177]

---

[174] **(U)** Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.
[175] **(U)** Eugene Rumer, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.
[176] **(U)** *Ibid.*
[177] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

(U) More recent social media activity attendant to the 2018 midterm elections indicates ongoing influence operations emanating from Russia. A September 2018 criminal complaint brought by the U.S. Attorney's Office for the Eastern District of Virginia against Elena Alekseevna Khusyaynova, an employee of the IRA who allegedly served as the chief accountant for the IRA, alleges that Khusyaynova sought to "interfere with U.S. political and electoral processes, including the 2018 U.S. elections."[178]

[redacted]

VII. (U) IRA USE OF SOCIAL MEDIA BY PLATFORM

(U) Facebook. Russia's influence operatives have found appeal in the cost-effectiveness of Facebook pages as a targeted communications medium. Data provided to the Committee by Facebook indicates that the IRA used to its advantage many of Facebook's features, beyond purchased advertising and pages, including the "events," messenger," and "stickers" features. The IRA also exploited Instagram—a photo- and video-sharing social networking service owned by Facebook.

(U) The first specific public warning about Russian activity on the Facebook platform came in September 2017, when Facebook announced the discovery of "approximately $100,000 in ad spending from June of 2015 to May of 2017—associated with roughly 3,000 ads—that was

[178] **(U)** Indictment, *United States v. Elena Alekseevna Khusyaynova,* Case 1:18-MJ-464 (E.D. Va. Sept. 28, 2018).
[179] [redacted]
[180] **(U)** *Ibid.*
[181] [redacted]

connected to about 470 inauthentic accounts and pages in violation of [Facebook's] policies."[182] Though not explicitly identified by Facebook at the time, the platform later attributed the subject accounts, pages, and advertisements to the IRA. Ongoing scrutiny of activity on its platform eventually led Facebook to a significantly larger body of non-advertisement content ("organic activity") that originated from these same IRA accounts. This content had been engineered to appear American. Facebook's initial discovery of the IRA-purchased advertisements was an essential first step in uncovering the IRA's 2016 information warfare campaign.

(U) Facebook Advertisements

(U) The Committee's analysis of the IRA-purchased advertisements indicates that the vast majority neither mention expressly the U.S. presidential election, nor explicitly advocate voting for or against a particular presidential candidate. Roughly five percent of the advertisements viewed prior to the election (77 of 1,519) included text referencing Hillary Clinton or Donald Trump. Forty of the post-election advertisements tied to the IRA referenced one of these candidates. The Committee found the content of these advertisements to be substantially consistent with Facebook's public statements that the advertisements overwhelmingly pertained to divisive and inflammatory U.S. social issues. The subject of these advertisements spanned the ideological and political spectrum, ranging from race, sexuality, and gender identity, to immigration and Second Amendment rights. A number of the advertisements encouraged Facebook users to follow IRA-created pages dedicated to these issues, from which the IRA could manufacture and disseminate organic content on any number of politically charged subjects directly to their page followers. According to Committee analysis of materials provided by Facebook, almost all the advertisements were purchased with Russian rubles.

(U) Facebook estimates that 11.4 million people in the United States saw at least one of the 3,393 advertisements ultimately determined to have been purchased by the IRA.[183] Modelling conducted by Facebook indicates that 44 percent of the total user views of these advertisements ("impressions") occurred before the election on November 8, 2016, with 56 percent of the impressions taking place after the election. Roughly 25 percent of the ads were never seen by anyone.[184]

(U) The IRA used Facebook's geographic targeting feature to channel advertisements to intended audiences in specific U.S. locations. About 25 percent of the advertisements purchased by the IRA were targeted down to the state, city, or in some instances, university level. Specific content narratives emerge in connection with targeted locations. For instance, Michigan and Wisconsin (32 and 55 pre-election advertisements, respectively) were targeted with

---

[182] **(U)** Alex Stamos, "An Update on Information Operations on Facebook," Facebook, September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/.
[183] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.
[184] **(U)** *Ibid.*

advertisements overwhelmingly focused on the subject of police brutality. Facebook indicates that the IRA did not leverage the platform's Custom Audiences tool, which would have entailed uploading or importing an externally held list of advertisement targets or contact data, revealing the IRA's efforts were not as sophisticated or potentially effective as they could have been.[185]

(U) IRA-Generated Facebook Content

(U) While early media reporting on the IRA's Facebook activity focused on purchased advertising, the organic content generated by IRA influence operatives on their Facebook pages far surpassed the volume of targeted advertisements. That IRA organic content reached a significantly larger U.S. audience.

(U) Facebook's initial public disclosures about IRA activity identified 470 pages and accounts as originating with the IRA. The dataset furnished to the Committee includes over 60,000 unique organic posts from 81 of the pages Facebook associated with the IRA. An estimated 3.3 million Facebook users followed IRA-backed pages, and these pages are the predicate for 76.5 million user interactions, or "engagements," including 30.4 million shares, 37.6 million likes, 3.3 million comments, and 5.2 million reactions. Facebook estimates that as many as 126 million Americans on the social media platform came into contact with content manufactured and disseminated by the IRA, via its Facebook pages, at some point between 2015 and 2017. Using contrived personas and organizations, IRA page administrators masqueraded as proponents and advocates for positions on an array of sensitive social issues. The IRA's Facebook effort countenanced the full spectrum of American politics, and included content and pages directed at politically right-leaning perspectives on immigration policy, the Second Amendment, and Southern culture, as well as content and pages directed at left-leaning perspectives on police brutality, race, and sexual identity.

(U) Demonstrative of the range of themes the IRA targeted on its Facebook pages, the 10 most active IRA-administered Facebook pages include: "Stop A.I." (an abbreviation for "Stop All Invaders," the page was focused on illegal immigration); "Being Patriotic" (right-leaning themes, including Second Amendment rights); "Blacktivist" (targeted at African-Americans, and focused on African-American cultural issues and police brutality); "Heart of Texas" (right-leaning themes and Texas secession); "United Muslims of America" (targeted at refugee rights and religious freedom); "Brown Power" (targeted at Latino heritage and immigrant rights); "South United" (focused on Southern culture, conservative issues); "BM" (racial equality and police brutality); "LGBT United" (sexual and gender identity rights); and "Army of Jesus" (conservative, Christian themes). "BM" was a replacement page for the IRA's "Black Matters US" page, which Facebook took down in 2016. The IRA used the BM Facebook page to direct users to the Black Matters US website.[186]

---

[185] **(U)** *Ibid.*

[186] **(U)** Craig Timberg and Tony Romm, "New report of Russian disinformation prepared for the Senate, shows the operation's scale and sweep," *Washington Post*, December 17, 2018.

(U) The IRA influence operatives responsible for these pages created fake online personas with a specific, readily discernible social agendas in order to attract similarly minded Facebook users. The operatives then used divisive content to anger and enrage the curated audience. The findings of the TAG study lead by Phil Howard and John Kelly explain the strategy behind the IRA's Facebook pages:

> *The IRA messaging [had] two strategies. The first involved appealing to the narratives common within a specific group, such as supporting veterans and police, or pride in race and heritage, as a clickbait strategy to drive traffic to the Facebook and Instagram pages the IRA set up. . . . Then the pages posted content that intended to elicit outrage from these groups.*[187]

(U) The IRA's development of Facebook pages and cultivation of followers was painstaking and deliberate. This resulted in the IRA creating top-performing pages that enabled sustained, long-term interaction with Americans on the very issues that drive Americans apart. The "Stop A.I." page eventually attracted nearly 12.5 million engagements, while the "Blacktivist" page garnered almost 11.2 million.

(U) The IRA's Facebook pages were not just channels for disseminating content across the social media platform. The IRA also used its Facebook presence to provoke real world events, including protests, rallies, and spontaneous public gatherings or "flashmobs." Facebook identified at least 130 events that were promoted on its platform as a result of IRA activity. These events were promoted by, and attributed to, 13 of the IRA's Facebook pages. Approximately 338,300 genuine Facebook user accounts engaged with content promoting these events. 62,500 Facebook users indicated their intention to attend the event, while another 25,800 users evinced interest in the event.[188]

(U) An early example of the IRA's experimentation with social media and real world events occurred in the spring of 2015, when IRA operatives attempted to induce a mass gathering in New York City by offering free hot dogs. According to the findings of an investigation into the IRA by Russian media outlet RosBiznesKonsalting (RBC), the success in attracting unwitting Americans to the IRA's promotion of the "event" on Facebook prompted the IRA's operatives to begin using the social media platform's "events" feature much more proactively. The RBC report concluded, "From this day, almost a year and a half before the election of the

---

[187] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[188] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.

US President, the 'trolls' began full-fledged work in American society."[189] The RBC investigation assesses that the IRA eventually spent about $80,000 to support 100 U.S. activists, who organized 40 different protests across the United States.[190]

(U) Over the course of 2016, IRA influence operatives trained particular focus on agitating political events and protests in the United States. One August 20, 2016, event promoted by the "Being Patriotic" page (over 216,000 followers) attempted to instigate flashmobs across Florida in support of Republican candidate for president, Donald Trump. Actual events promoted as "Florida Goes Trump" gatherings took place in Ft. Lauderdale and Coral Springs, Florida.[191]

(U) A May 2016, real world event that took place in Texas illustrates the IRA's ideological flexibility, command of American politics, and willingness to exploit the country's most divisive fault lines. As publicly detailed by the Committee during a November 1, 2017 hearing, IRA influence operatives used the Facebook page, "Heart of Texas" to promote a protest in opposition to Islam, to occur in front of the Islamic Da'wah Center in Houston, Texas. "Heart of Texas," which eventually attracted over 250,000 followers, used targeted advertisements to implore its supporters to attend a "Stop Islamization of Texas" event, slated for noon, May 21, 2016. Simultaneously, IRA operatives used the IRA's "United Muslims for America" Facebook page and its connection to over 325,000 followers to promote a second event, to be held at the same time, at exactly the same Islamic Da'wah Center in Houston. Again, using purchased advertisements, the IRA influence operatives behind the "United Muslims for America" page beseeched its supporters to demonstrate in front of the Islamic Da'wah Center—this time, in order to "Save Islamic Knowledge." In neither instance was the existence of a counter-protest mentioned in the content of the purchased advertisement.

(U) The competing events were covered live by local news agencies, and according to the Texas Tribune, interactions between the two protests escalated into confrontation and verbal attacks. The total cost for the IRA's campaign to advertise and promote the concomitant events was $200, and the entire operation was conducted from the confines of the IRA's headquarters in Saint Petersburg. Social media researcher John Kelly characterized the IRA's operational intent as "kind of like arming two sides in a civil war so you can get them to fight themselves before you go and have to worry about them."[192]

(U) Analysis of the dataset made available to the Committee indicates that IRA operatives also took advantage of the Facebook recommendation algorithm, an assessment

---

[189] **(U)** *See* Hannah Levintova, "Russian Journalists Just Published a Bombshell Investigation About a Kremlin-Linked 'Troll Factory,'" *Mother Jones*, October 18, 2017. Original report in Russian available at https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1.

[190] **(U)** *Ibid.*

[191] **(U)** Ben Collins, Gideon Resnick, et al., "Exclusive: Russians Appear to Use Facebook to Push Trump Rallies in 17 U.S. Cities," *The Daily Beast,* September 20, 2017.

[192] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

Facebook officials have corroborated. When asked by Senator Susan Collins whether Facebook's recommendation engine ever suggested content created by IRA operatives to Facebook users, Facebook officials admitted that "This happened in some cases," adding that IRA content was "sometimes recommended when people followed similar pages."[193]

(U) In order to maximize the speed and scale of Russia's information warfare campaign, IRA operatives utilized the Facebook platform, and almost the entirety of its suite of features and capabilities, exactly as it was engineered to be used.

(U) Instagram. The use of Instagram by the IRA, and Instagram's centrality as a channel for disseminating disinformation and societally divisive content, has escaped much of the media and public attention that has focused on other social media platforms.

(U) IRA influence operatives in St. Petersburg, Russia, first posted on Instagram in January 2015—at the same time as their first posts on Facebook. Ultimately, IRA activity and engagement with Americans through Instagram accounts dramatically eclipsed the comparable interaction achieved through Facebook pages.[194]

(U) Data provided to the Committee indicates that the IRA used 133 Instagram accounts to publish over 116,000 posts. By comparison, the IRA used Facebook pages to publish over 60,000 posts. Engagement with fellow platform users was also significantly greater on Instagram, where IRA accounts accumulated 3.3 million followers and generated 187 million total engagements. By comparison, the IRA's Facebook page audience of 3.3 million produced 76 million virtual interactions. As Renee DiResta assessed in testimony to the Committee, "Instagram dramatically outperformed Facebook in terms of reach and in terms of likes and in terms of engagement, on a per-post [basis]."[195]

(U) The tactics IRA operatives used on the Instagram platform were consistent with those employed on the Facebook platform. The IRA's Instagram accounts focused on both the political left and right in America, and exploited the social, political, and cultural issues most likely to incite impassioned response across the ideological spectrum. Significantly, a discernible emphasis on targeting African-Americans emerges from analysis of the IRA's Instagram activity.[196]

---

[193] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.

[194] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[195] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[196] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

(U) The size, scope, and intended U.S. audience of the IRA's Instagram activity is reflected in the account names of the top 10 IRA Instagram accounts by follower numbers:

- "@Blackstagram_" targeted African-American cultural issues, amassed over 300,000 followers, and generated over 28 million interactions on the Instagram platform.
- "@american.veterans" was aimed at patriotic, conservative audiences, collected 215,680 followers, and generated nearly 18.5 million engagements.
- "@sincerely_black_" built a following of 196,754 Instagram users.
- "@rainbow_nation_us" emphasized sexual and gender identity rights and built a following of 156,465 users.
- "@afrokingdom_" had 150,511 followers on Instagram.
- "@_american.made" focused on conservative and politically right-leaning issues, including Second Amendment freedoms, and built a following of 135,008.
- "@pray4police" amassed 127,853 followers.
- "@feminism_tag" had 126,605 followers.
- "@_black_business" built a following of 121,861 Instagram users.
- "@cop_block_us" was followed by 109,648 Instagram users.

(U) In total, over the course of more than two years spent as an instrument for foreign influence operations, 12 of the IRA's Instagram accounts amassed over 100,000 followers, and nearly half of the IRA's 133 Instagram accounts each had more than 10,000 followers. On the basis of engagement and audience following measures, the Instagram social media platform was the most effective tool used by the IRA to conduct its information operations campaign.[197]

(U) Despite the high Instagram engagement numbers reported to the Committee through the TAG social media research effort, in testimony to the Committee, Facebook representatives indicated that Instagram content reached just 20 million users. In relation to the Facebook estimate, the published findings of the working group led by TAG researcher Renee DiResta contest that "the Instagram number is likely lower than it should be" and advocate for additional

[197] **(U)** The IRA also purchased targeted advertisements on Instagram. The data associated with these purchases was included in the total Facebook advertisements production to the Committee in the fall of 2017. The 3,393 advertisements purchased by the IRA included both Facebook and Instagram buys. Because the Facebook and Instagram buys were produced together, the Committee's analysis has also grouped them together, and these advertisements are collectively addressed in the above treatment of the IRA's use of Facebook advertisements.

research on Instagram content and activities.[198] Additional data and analysis concerning IRA activity on Instagram are required to resolve this discrepancy.

(U) Twitter. Though Twitter has fewer U.S. users than Facebook (68 million monthly active users on Twitter in the United States compared to 214 million Facebook users), Twitter is an extremely attractive platform for malicious influence operations like those carried out by the IRA due to its speed and reach. In 2017 testimony to the Committee, disinformation expert Thomas Rid identified Twitter as one of the more influential "unwitting agents" of Russian active measures.[199] Available data on the IRA's activity on the Twitter platform reinforces this assessment. As of September 2018, Twitter had uncovered over 3,800 accounts tied to the IRA.[200] According to data provided to the Committee by Twitter, those accounts generated nearly 8.5 million tweets, resulting in 72 million engagements on the basis of that original content.[201,202] More than half (57 percent) of the IRA's posts on Twitter were in Russian, while over one-third (36 percent) were in English.[203] Twitter estimates that in total, 1.4 million users engaged with tweets originating with the IRA.

(U) The activity of IRA influence operatives on Twitter outpaced the IRA's use of Facebook and Instagram. TAG members Phil Howard and John Kelly noted in their publicly released analysis of IRA activity:

> *The volume of Twitter posts made available to us is much larger than the volume of Facebook ads, Facebook posts, and Instagram posts. The average monthly*

---

[198] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[199] **(U)** Thomas Rid, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[200] **(U)** Twitter provided the Committee with a significant amount of data (including tweet content, handle names, engagement activity, and other metadata) for each of the over 3,800 accounts they identified as being linked to the IRA. That unique dataset was provided in installments that began in the fall of 2017. In October 2018, Twitter published a large archive of this information for the public to examine, including all tweets from the IRA-linked accounts. The Committee commends Twitter for its decision to publicize the data from these accounts and urges Twitter leadership to continue to make available to the public any future influence operation activities. The Committee urges other social media companies to take comparable steps to increase transparency and allow the public, outside researchers, investigators, and media to more fully examine the scope and scale of these types of influence operations as a matter of corporate responsibility and public service.

[201] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[202] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[203] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

Twitter post volume is over fifty thousand tweets per month, while the average monthly volume of Facebook ads, Facebook posts, and Instagram posts is in the hundreds to low thousands, never exceeding the six thousand mark.[204]

(U) It appears from the data that the IRA, or a predecessor of the organization, began posting on Twitter in 2009, mostly in the Russian language and with a focus on the domestic Russian audience. These accounts continued to target Russia-internal issues and audiences until they were closed down in 2017.[205] It wasn't until 2013 that accounts tied to the IRA began to target a U.S. audience with English language tweets.[206]

(U) According to Phil Howard and John Kelly, the activity on Twitter constitutes the IRA's first use of a social media platform to conduct information warfare against the United States. The IRA effort shortly thereafter incorporated additional social media platforms including YouTube, Instagram, and Facebook:

It appears that the IRA initially targeted the US public using Twitter, which it had used domestically in Russia for several years. But as the IRA ramped up US operations toward the end of 2014, this dataset suggests that the IRA began leveraging other platforms in sequence: YouTube (here measured via Twitter citations of YouTube content), Instagram, and lastly Facebook.[207]

(U) Initially, the IRA's Twitter activity targeting a U.S. audience was constrained to a relatively low operational tempo, approximating an initial test phase. By 2014 and 2015, however, the IRA's U.S.-focused efforts had significantly intensified. The elevated level of activity was sustained all the way through the 2016 presidential election campaign period, and spiked with an anomalous peak in activity immediately following the election, in November 2016. By mid-2017, U.S.-focused IRA activity on Twitter surpassed the IRA's domestic, Russia-focused information operations on the platform.[208] All Twitter accounts known to be associated with the IRA were suspended by the company by late 2017, and data associated with these accounts was turned over to the Committee.

(U) The data furnished to the Committee suggests IRA influence operatives probably used automated accounts to amplify payload content by tweeting and retweeting selected Twitter messaging. DiResta elaborated on the IRA's use of automated bots: "In the course of a similarity analysis we discovered still-active bots that were likely part of a commercially acquired or repurposed botnet."[209]

---

[204] **(U)** *Ibid.*
[205] **(U)** *Ibid.*
[206] **(U)** *Ibid.*
[207] **(U)** *Ibid.*
[208] **(U)** *Ibid.*
[209] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

(U) In addition to the Twitter accounts identified by the company as tied to the IRA, Twitter uncovered 50,258 automated accounts that they believe to be tied to Russia. These bot accounts were issuing tweets containing election-related content during the 2016 U.S. presidential election campaign period.[210] Although Twitter could not definitively link these bot accounts directly to the IRA, they illustrate the vulnerability of U.S. democratic processes to automated influence attacks, and the scale of the effort emanating from Russia to exploit that vulnerability. The coordinated activity of multiple bot accounts on social media represents an additional element of the foreign influence threat. According to platform monitoring reports prepared for officials in the United Kingdom, an estimated 2,800 automated accounts believed linked to Russia posted content concerning the 2018 poison attack on Sergei Skripal and his daughter in Salisbury, England, in an effort to provoke uncertainty over culpability for the attack.[211]

(U) The IRA's influence operatives dedicated significant effort to repurposing existing fake Twitter accounts, and creating new ones, that appeared to be owned by Americans. These accounts were used to build American audiences, accrue account followers, and amplify and spread content produced by the IRA. An analysis of the IRA's Twitter accounts illuminates the strategy and objectives behind its Twitter activity. Clemson researchers, led by Darren Linvill and Patrick Warren, collected all of the tweets from all the IRA-linked accounts between June 19, 2015, and December 31, 2017.[212] After removing from the sample all non-English accounts and those that did not tweet at all, the team was left with 1.875 million tweets associated with 1,311 IRA usernames.

(U) After conducting an analysis of all the content that IRA influence operatives manufactured, the Clemson researchers separated the IRA-affiliated accounts into five categories of social media platform activity. According to this analysis, "Within each type, accounts were used consistently, but the behavior across types was radically different." Characterizing the IRA Twitter effort as "industrial," the researchers described the campaign as "mass produced from a system of interchangeable parts, where each class of part fulfilled a specialized function."[213] The researchers named the account types: Right Troll, Left Troll, Newsfeed, Hashtag Gamer, and Fearmonger.

- **(U) Right Troll.** This was the largest and most active group of IRA-affiliated accounts. The 617 Right Troll Twitter accounts tweeted 663,740 times and cultivated nearly a million total followers. Clemson researchers characterized these accounts as focused on spreading "nativist and right-leaning populist messages." They strongly supported the

[210] **(U)** Jack Dorsey, Hearing before the Senate Select Committee on Intelligence, September 5, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[211] **(U)** Deborah Haynes, "Skripal attack: 2,800 Russian bots 'sowed confusion after poison attacks,'" *The Times UK*, March 24, 2018.
[212] **(U)** Darren Linvill and John Walker, "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building," Clemson University, https://www.rcmediafreedom.eu/Publications/Academic-sources/Troll-Factories-The-Internet-Research-Agency-and-State-Sponsored-Agenda-Building.
[213] **(U)** *Ibid.*

candidacy of Donald Trump, employed the #MAGA hashtag, and attacked Democrats. Although nominally "conservative," Clemson researchers found that the IRA accounts rarely promoted characteristically conservative positions on issues such as taxes, regulation, and abortion, and instead focused on messaging derisive of Republicans deemed "too moderate" (including at the time Senators John McCain and Lindsey Graham).[214] The accounts generally featured very little in the way of identifying information, but frequently used profile pictures of "attractive, young women."

- **(U) Left Troll.** The second largest classification of IRA-affiliated Twitter accounts, consisting of around 230 Twitter profiles that generated 405,549 tweets, was Left Troll. The focus of the Left Troll Twitter accounts was primarily issues relating to cultural identity, including gender, sexual, and religious identity. Left Troll accounts, however, were acutely focused on racial identity and targeting African-Americans with messaging and narratives that mimicked the substance of prominent U.S. activist movements like Black Lives Matter. Left Troll accounts directed derisive content toward moderate Democrat politicians. These accounts targeted Hillary Clinton with content designed to undermine her presidential campaign and erode her support on the U.S. political left.

- **(U) News Feed.** Designed to appear to be local news aggregators in the United States, News Feed Twitter accounts would post links to legitimate news sources and tweet about issues of local interest. Examples of the IRA's news-oriented influence operative accounts on Twitter include @OnlineMemphis and @TodayPittsburgh. About 54 IRA accounts share the characteristics of this classification of Twitter profile, and they were responsible for 567,846 tweets.

- **(U) Hashtag Gamer.** More than 100 of the IRA's Twitter accounts were focused almost exclusively on playing "hashtag games," a word game popular among Twitter users. At times, these games were overtly political and engineered to incite reactions on divisive social issues from both the left and the right ends of the ideological spectrum.

- **(U) Fearmonger.** Finally, the IRA's 122 Fearmonger Twitter accounts were specifically dedicated to furthering the spread of a hoax concerning poisoned turkeys during the Thanksgiving holiday of 2014. The Fearmonger Twitter accounts tweeted over 10,000 times.

(U) The IRA's influence operatives coordinated across these Twitter account classifications to attack and defend both sides of socially divisive issues, particularly with respect to race relations and cultural divisions. An example of the IRA's ability to capitalize on both sides of a public debate can be found in the issue of NFL players kneeling in protest of police brutality and racism. Twitter accounts tied to the IRA from both the left and right side of the ideological spectrum used the topic to channel inflammatory content toward targeted, and ideologically like-minded, audiences. A Left Troll account, @wokeluisa, tweeted in support of

[214] **(U)** Jim Galloway, "Clemson researchers crack open a Russian troll factory," *Associated Press,* August 7, 2018.

Colin Kaepernick and the NFL protests on March 13, 2018, prompting 37,000 forwarded retweets. Simultaneous to this, and in the direction of the ideologically opposite audience, @BarbaraForTrump, a Right Troll account, was tweeting content hostile to the protests.[215]

(U) The Twitter data provided to the Committee shows that the IRA's influence operatives used multiple false personas to incite division and antipathy along a host of ideological fissures, simultaneously taking and attacking all sides of the arguments, all from the same internet protocol (IP) address. As TAG consultant John Kelly uncovered:

> *It was literally the same computer that was registering and operating the America accounts, pretending to be right and pretending to be left. So imagine it's the same guy, and the same people, and they got their two little marionette things with their puppets dancing on either end of a string. And they are playing them together. They are inhabiting both sides and figuring out ways to play them off against each other.*[216]

(U) As was the case with IRA activity on Facebook and Instagram, influence operatives based in Russia spent months developing fake Twitter personas and cultivating networks of supporters and followers among sympathetic and agreeable Americans. For example, 118 accounts secured more than 10,000 followers, and six accounts built followings of over 100,000 Twitter users.

(U) One of the IRA's most successful fake Twitter profiles was the @TEN_GOP account. By the time Twitter shut down the @TEN_GOP account in August 2017, it had amassed over 150,000 followers. By contrast, the legitimate Twitter account for the Tennessee Republican Party (@tngop) had 13,400 followers. Despite three separate requests by the actual Tennessee Republican Party organization to take down the account, @TEN_GOP was successful in deceptively injecting its inflammatory content into the political mainstream throughout 2016 and 2017.[217] Quotes and content from IRA influence operatives using the @TEN_GOP Twitter account were widely cited in press articles and mainstream media, and retweeted by celebrities and politicians, including several Trump campaign affiliates, including Donald Trump Jr., Kellyanne Conway, and Lieutenant General Michael Flynn (U.S. Army, retired).[218]

(U) As Clint Watts has described, influence operations like the @TEN_GOP effort can be extremely successful once the content filters into the mainstream press: "If you can get

---

[215] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[216] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[217] **(U)** Kevin Collier, "Twitter Was Warned Repeatedly About This Fake Account Run By a Russian Troll Farm and Refused to Take it Down," *BuzzFeed News,* October 18, 2017.

[218] **(U)** Philip Bump, "At least five people close to Trump engaged with Russian Twitter trolls from 2015 to 2017," *Washington Post,* November 2, 2017.

indigenous content, turn that into a conspiracy, and filter that into the mainstream media, that's a textbook case. . . . As an information warfare missile, that was a direct hit."[219]

(U) Another example of an effective IRA influence operation carried out on Twitter was conducted using the @Jenn_Abrams account. The persona associated with @Jenn_Abrams had accounts on multiple platforms, but most notably amassed over 80,000 followers on Twitter. This persona would tweet about everything from segregation to the futility of political correctness, and she would eventually be cited by more than 40 U.S. journalists before being taken down by Twitter in late 2017. John Kelly was among those following @Jenn_Abrams on Twitter. In testimony during a closed Committee hearing, Kelly described the ability of IRA influence operatives to infiltrate entire swaths of the political ecosystem on Twitter, of either ideological persuasion, using the persona:

> *Now . . . we're lighting up Jenn Abrams' account and all of the people following her are lit up. . . . So she had almost the entirety of the activist right, a good bit of the activist left, because remember the IRA has puppets on both sides – they are actually the same people running the machines – building her credibility. And then down below she's managed to make inroads and followership among the mainstream conservative part of that network, and she's even got a few of the mainstream liberal folks following her.*[220]

(U) The IRA was also successful using Twitter accounts feigning left-leaning ideological sentiment. An example cited by Laura Rosenberger in testimony to the Committee, @wokeluisa – which was still active in 2018 and had over 50,000 followers – claimed to be an African-American political science major in New York. Content produced under the guise of this persona would eventually appear "in more than two dozen news stories from outlets such as BBC, USA Today, Time, Wired, Huffington Post, and BET."[221]

(U) While original content creation was a preoccupation largely reserved for IRA operatives on Facebook and Instagram, the IRA's Twitter accounts were used to amplify events and promote the dissemination of content already existing on social media. This distinction notwithstanding, the Twitter platform was an integral tool for IRA operatives. As Renee DiResta detailed in her team's report:

> *Our impression of the IRA's Twitter operation is that it was largely opportunistic real-time chatter; a collection of accounts, for example, regularly played hashtag games. There was a substantial amount of retweeting. By contrast, Facebook and Instagram were used to develop deeper relationships, to create a collection of*

[219] **(U)** Brandy Zadrozny and Ben Collins, "How a right-wing troll and a Russian Twitter account created 2016's biggest voter fraud story," *NBC News,* October 30, 2018.
[220] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.
[221] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

substantive cultural media pages dedicated to continual reinforcement of in-group and out-group ideals for targeted audiences. Twitter was, however, a part of the cross-platform brand building tactic; several of the Facebook, Instagram, Tumblr, and Reddit pages had associated Twitter accounts.[222]

(U) In a similar conclusion outlining the importance of Twitter to the IRA's effort to influence the thinking of Americans, Phil Howard and John Kelly found the following:

...the IRA Twitter data shows a long and successful campaign that resulted in false accounts being effectively woven into the fabric of online US political conversations right up until their suspension. These embedded assets each targeted specific audiences they sought to manipulate and radicalize, with some gaining meaningful influence in online communities after months of behavior designed to blend their activities with those of authentic and highly engaged US users.[223]

(U) Google. To a lesser but still critically important extent, Google and its numerous subsidiary platforms were also utilized and exploited by the IRA to the same end, in distinct ways. According to data provided to the Committee by Google, and additional public disclosures, numerous Google-affiliated platforms were utilized by IRA operatives, including YouTube, Google+, Gmail, Google's various advertisement platforms, Search, and Google Voice.

(U) There is little evidence that the IRA's operational efforts were as reliant on Google's products as they were on Facebook, Instagram, or Twitter to execute the most outwardly visible aspects of their information warfare campaign. The design, nature, and intended use of most Google products probably lies at the heart of this imbalance. Although Gmail accounts were used by IRA operatives to establish account profiles on other social media platforms, Google's products are generally not conducive to the rapid, expansive public dissemination of content that makes Facebook and Twitter attractive to influence operatives. Google's then-Senior Vice President and General Counsel, Kent Walker, testified to the Committee in November 2017, "Google's products didn't lend themselves to the kind of micro-targeting or viral dissemination that these [IRA] actors seemed to prefer."[224]

---

[222] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[223] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[224] **(U)** Kent Walker, Hearing before the Senate Select Committee on Intelligence November 1, 2017, available at https://www.intelligence.senate.gov/hearings/open.

(U) IRA operatives were not, however, entirely absent from Google and its subsidiaries. Among the Google products that contributed to the wide-ranging character of the IRA's information warfare campaign, YouTube was by far the most utilized by operatives. In addition to IRA activity on YouTube, Google also uncovered evidence that Russian operatives utilized some of the company's advertisement products and services during the 2016 election campaign period. Using Gmail accounts connected to the IRA, influence operatives reportedly purchased $4,700 worth of search advertisements and more traditional display advertisements in relation to the 2016 presidential election.[225]

(U) Americans also engaged with a separate $53,000 worth of politically themed advertisements that either had a connection to a Russian internet or physical building address, or had been purchased with Russian rubles. It is unclear, however, whether these ads are tied to the Russian government. The content of these ads spans the political spectrum, and features messages alternately disparaging and supporting candidates from both major political parties, as well as the then incumbent U.S. President. The total amount of advertisement spending related to the election on Google AdWords was about $270 million, making the Russia-linked purchases on the Google platform miniscule by comparison. Gmail addresses and other Google applications were also utilized to establish accounts on both Facebook and Twitter. According to Renee DiResta, "YouTube, G+, and other properties were leveraged to either host content or to support personas."[226]

(U) As a tool of information warfare, the Google "Search" application presents a distinct method for broadly disseminating disinformation. Google's search engine is by far the most utilized on the internet, however Google has been criticized for its failure to address issues with its PageRank algorithm. Periodically, particularly in the context of fast breaking news, Google's algorithm can elevate extremist content or disinformation to the top of certain searches. Days after the 2016 presidential election, a falsified media account of President-elect Donald Trump having won the popular vote briefly ranked higher than stories that accurately reflected the U.S. popular vote result.[227]

(U) Google was quick in responding to and addressing the misleading 2016 popular vote search results, but the example illustrates that the Google platform's search results feature is not impervious to manipulation designed to spread deceptive and misleading information. Public statements by Google representatives emphasize that the company realizes no business interest or advantage in the selective promotion of falsified news stories, extremist content, and conspiracy theories.

(U) As Laura Rosenberger testified to the Committee, "Another way the Russian government distorts the information space is through manipulating search results. Just Google

---

[225] **(U)** *Ibid.*

[226] **(U)** Renee DiResta, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[227] **(U)** Philip Bump, "Google's top news link for 'final election results' goes to a fake news site with false numbers," *Washington Post,* November 14, 2016.

any geopolitical issue of significance to Moscow—MH-17, the White Helmets, the Novichok poisonings in the UK—and you will be served up a set of top results consisting of outlandish conspiracy theories emanating from Russia."[228]

(U) Private sector entities around the world dedicate sustained effort to manipulating the Google Search algorithm for commercial benefit. "Search-engine optimization," which entails maximizing the likelihood of favored content appearing among the highest ranked query results, is a standard marketing firm capability routinely used in the promotion of businesses and products. The IRA's 2016 information warfare campaign featured some of the same capabilities. According to the Department of Justice indictment, the IRA devoted an entire department to search-engine optimization, the objective of which was the elevation of the IRA's content in the search results of Americans, in furtherance of the IRA's 2016 information warfare campaign.[229]

(U) YouTube. Distinct from Facebook and Twitter, the YouTube platform is not independently conducive to rapid and expansive content sharing. Achieving the "viral" spread of YouTube videos generally entails capitalizing on the reach and magnitude of Facebook and Twitter networks to spread links to the video hosted on YouTube.

(U) Data provided to the Committee by YouTube concerning IRA-associated content and accounts indicates that IRA influence operatives began posting videos to YouTube as early as September 2015. More than 1,100 videos, or 43 hours of content, were eventually posted on 17 YouTube channels the IRA established. Two of these channels were overtly political in character, and focused on the 2016 U.S. presidential election.[230]

(U) The overwhelming preponderance of the video content posted to the IRA's YouTube channels was aimed directly at the African-American population. Most of the videos pertained to police brutality and the activist efforts of the Black Lives Matter organization. Posted to 10 of the IRA's YouTube channels, were 1,063 videos—or roughly 96 percent of the IRA content—dedicated to issues of race and police brutality. The names of the IRA's YouTube channels were consistent with the posted video content and included "Black Matters," "BlackToLive," "Cop Block US," "Don't Shoot," and "PoliceState." The content of the videos posted to those channels exploits issues of extraordinary sensitivity inside the African-American community. It is difficult to reconcile this fact with public testimony to the Committee by a Google representative that, "The videos were not targeted to any particular sector of the US population as that's not feasible on YouTube."[231]

---

[228] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[229] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[230] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[231] **(U)** Kent Walker, Hearing before the Senate Select Committee on Intelligence November 1, 2017, available at https://www.intelligence.senate.gov/hearings/open.

(U) Only 25 videos posted to the IRA's YouTube channels featured election-related keywords in the title. All of the IRA's politically-oriented videos were thematically opposed to the Democrat candidate for president, Hillary Clinton. Some of the videos featured expressly voter suppressive content intended to dissuade African-American voters from participating in the 2016 presidential election, while others encouraged African-Americans to vote for Jill Stein.

(U) YouTube continues to be the propaganda vehicle of choice for Russia's state-sponsored news organization, RT (formerly Russia Today). As of February 2019, RT had nearly 3.3 million global subscribers on its YouTube channel. In 2013, RT was the first self-described "news channel" to break 1 billion views on YouTube, and in 2017, RT's YouTube channel accumulated its five billionth view. RT's social media presence and activities were outlined in the January 6, 2017 Intelligence Community Assessment, in an annex to the unclassified version of the report.[232]

(U) Reddit. IRA influence operatives were active on the Reddit platform during the 2016 presidential election campaign period, in part it appears, to test audience reaction to disinformation and influence campaign content before its dissemination through other social media platform channels.

(U) Motivated by the fall 2017 revelations of significant IRA activity on the Facebook and Twitter platforms, Reddit conducted an internal investigation into whether IRA activity had taken place on its platform. The results of Reddit's internal investigation, which were shared with the Committee, indicate that IRA influence operatives were active on the platform and attempted to engage with American Reddit users. Internal investigators characterized 944 Reddit accounts as "suspicious," imparting that investigators judged there was a "high probability" that the accounts were linked to the IRA.[233] Analysis of the accounts indicates that nearly three-quarters (662 accounts) achieved zero karma points, indicative of minimal engagement by the broader Reddit user base.

(U) According to Reddit, the 944 evaluated accounts were responsible for around 14,000 posts. Of those posts that contained socially or politically divisive content, most were thematically focused on police brutality, issues of race, and the disparagement of Hillary Clinton. A Reddit account with the username Rubinjer, the most popular of the accounts Reddit investigators assessed as probably linked to the IRA, posted a video that falsely claimed to depict Hillary Clinton engaged in a sex act. The video, which was ultimately posted on a separate website dedicated to pornographic content and viewed more than 250,000 times, was created by the IRA's influence operatives.[234] The same Reddit account was used to promote a videogame titled Hilltendo, in which players maneuver an animated Hillary Clinton as the avatar deletes emails and evades FBI agents. IRA influence operatives attempted to achieve viral

---

[232] **(U)** ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," *Intelligence Community Assessment (Unclassified Version),* January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[233] **(U)** Reddit, Submission to SSCI, April 10, 2018.
[234] **(U)** Ben Collins, "Russia-Linked Account Pushed Fake Hillary Clinton Sex Video," *NBC News,* April 10, 2018.

dissemination of the video game across social media, weeks prior to the 2016 election.[235] IRA influence operatives also used Reddit as a platform for Russia-friendly narratives. As Laura Rosenberger testified to the Committee: "On Reddit, multiple IRA-generated memes posted to the 'r/funny' sub-reddit were targeted at discouraging United States support for Montenegrin-accession to NATO, attempting to portray Montenegrins either as free riders or as protestors resisting this move."[236]

(U) In Reddit's assessment, IRA information warfare activity on its platform was largely "unsuccessful in getting any traction." The company judges that most Russian-origin disinformation and influence content was either filtered out by the platform's moderators, or met with indifference by the broader Reddit user base. In an April 2018 statement, Reddit CEO, Steve Huffman, stated that the investigations had "shown that the efforts of [Reddit's] Trust and Safety Team and Anti-Evil teams are working," and that the "work of [Reddit] moderators and the healthy skepticism of [Reddit] communities" made Reddit a "difficult platform to manipulate."[237] Nevertheless, the largely anonymous and self-regulated nature of the Reddit platform makes it extremely difficult to diagnose and attribute foreign influence operations. This relative user autonomy and the dearth of information Reddit collects on its users make it probable that Reddit remains a testbed for foreign disinformation and influence campaigns.

(U) Tumblr. Following Facebook's September 2017 disclosures about IRA activity on the platform, Tumblr conducted an internal investigation to determine whether Russia-based operatives had also been active on Tumblr.[238] The ensuing investigation uncovered 84 accounts determined to be associated with the IRA. Most of the accounts were created in 2014 or 2015, and did not exhibit indications of automation. The IRA-associated Tumblr accounts generated about 100,000 posts, and were engaged significantly with authentic (non-IRA) user accounts on Tumblr. Tumblr estimates that IRA influence operatives used the platform to interact with 11.7 million unique U.S. users, and nearly 30 million unique users globally. Tumblr did not find any indication that IRA operatives purchased advertisements through the platform's advertising feature.[239]

(U) Tumblr's investigative findings indicate that content posted to the IRA's accounts was focused primarily on politics and divisive social issues. A discernible effort to focus content delivery toward African-Americans is evident in the Tumblr account names the IRA chose, and the content those accounts posted. Among the IRA's Tumblr profile names were:

---

[235] **(U)** Jose Pagliery and Donie O'Sullivan, "Russians released anti-Clinton video game weeks before election," *CNN Business*, March 8, 2018.

[236] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[237] **(U)** Steve Huffman, "Reddit's 2017 transparency report and suspect account findings," Reddit, April 10, 2018, https://www.reddit.com/r/announcements/comments/8bb85p/reddits_2017_transparency_report_and_suspect/

[238] **(U)** Tumblr is a New York-based social networking and micro-blogging site that was created in 2007, and eventually acquired by Verizon and placed under the umbrella subsidiary, Oath, Inc. (later, renamed Verizon Media).

[239] **(U)** SSCI staff interview with Oath/Tumblr on Russian influence, April 20, 2018.

"aaddictedtoblackk," "black-to-the-bones," "blackness-by-your-side," "blacknproud," and "bleepthepolice."[240] Jonathan Albright, a researcher at the Tow Center for Digital Journalism at Columbia University, is unequivocal in concluding that on Tumblr, the IRA's influence operatives deliberately focused on messaging young African-American with narratives and payload content: "The evidence we've collected shows a highly engaged and far-reaching Tumblr propaganda-op targeting mostly teenage and twenty-something African-Americans."[241]

(U) As was the case on other social media platforms, IRA influence operatives used Tumblr accounts to build audiences of like-minded Americans, into which they would sow socially and politically divisive content. As reported in *BuzzFeed*, a Tumblr account named "4mysquad," which was later revealed by Tumblr to be operated by the IRA, dealt almost exclusively with issues of sensitivity to the African-American community. On occasion, political content promoting the presidential campaign of Bernie Sanders, or criticizing Hillary Clinton was posted to this account. As an example, "4mysquad" posted a video of Clinton calling young black gang members "superpredators," which generated more 50,000 engagements with authentic Tumblr users.[242] Over time, however, the IRA's influence operatives took the messaging broadcast via the "4mysquad" Tumblr account further than the credulity of some users would allow. As one former follower of the account was quoted, after "4mysquad" began posting content promoting the presidential campaign of Donald Trump, "I unfollowed him and the thing that was a red flag was that it was supposedly a black liberal blog that at some point started rooting for Trump to win."[243]

(U) Tumblr shared the results of the 2017 internal investigation with federal law enforcement. In the fall of 2018, law enforcement reciprocally alerted Tumblr to potential IRA operational activity tied to the U.S. 2018 mid-term elections taking place on the platform. On the basis of this insight, Tumblr identified 112 accounts tied to what was identified as an influence operation, indicating that Russia-based influence operatives continue to exploit the Tumblr platform targeting the United States.[244]

(U) In addition to the internal investigation into IRA activities on Tumblr, Oath's security team also searched the company's other digitally-based platforms, uncovering 484 Yahoo email accounts associated with other publicly identified IRA account information. Most of the Yahoo email accounts were used to establish profiles and enable commenting on other social media platforms.[245] Oath's internal security investigation also uncovered a small number

---

[240] **(U)** Tumblr, "Public record of usernames linked to state-sponsored disinformation campaigns," March 23, 2018, https://staff.tumblr.com/post/180179385310/keeping-our-promise-to-be-transparent-about.

[241] **(U)** Craig Silverman, "Russian Trolls Ran Wild on Tumblr and the Company Refuses to Say Anything About It," *BuzzFeed News,* February 6, 2018.

[242] **(U)** *Ibid.*

[243] **(U)** *Ibid.*

[244] **(U)** Tumblr Staff, "Keeping our promise to be transparent about state-sponsored disinformation campaigns," Tumblr, November 16, 2018, https://staff.tumblr.com/post/180179385310/keeping-our-promise-to-be-transparent-about.

[245] **(U)** SSCI staff interview with Oath/Tumblr on Russian influence, April 20, 2018.

of accounts with some indications of association with the IRA on Flickr, a photo and video hosting service. Only four of the seven Flickr accounts investigators found associated with the IRA had posted images.[246]

(U) LinkedIn. LinkedIn discovered that IRA-linked activity occurred on the platform during the period of the 2016 presidential election. In the course of an internal investigation initiated after the fall 2017 Facebook disclosures, LinkedIn uncovered 91 accounts and five fake company pages believed to be tied to the IRA. Most of the accounts were established in 2015. About 24 of the accounts never posted content to the platform. Eighty percent of the content posted from these accounts generated no engagement from any other LinkedIn users. None of the accounts is known to have purchased ads or any promoted content on the platform.[247] However a common IRA approach involved establishing credibility by creating multiple social media accounts across an array of platforms, under the same falsified American persona.

(U) Though foreign influence operational activity on LinkedIn appears to be limited, the platform and its users are a significant target for foreign intelligence services. LinkedIn users submit, and make publicly accessible, significant personal and professional data in the pursuit of networking opportunities and to attract potential employers. This renders the platform a valuable source of information on an array of sensitive intelligence targets—including the identities of government employees, active duty military personnel, cleared defense contractors, and others. As Director of the U.S. National Counterintelligence and Security Center William Evanina has stated, LinkedIn "makes for a great venue for foreign adversaries to target not only individuals in the government, formers, former CIA folks, but academics, scientists, engineers, anything they want. It's the ultimate playground for (intelligence) collection."[248]

(U) Other Platforms. Medium, a popular online publishing platform, and Pinterest, a photo- and image-focused social media platform with over 250 million active users, both publicly acknowledged the discovery of IRA influence operative activity on their platforms. The Committee's TAG researchers also discovered IRA activity on other popular internet sites, including Vine, Gab, Meetup, VKontakte, and LiveJournal. Even browser extensions, music applications, and games, like Pokémon Go were incorporated into the IRA's influence operation.[249] As Renee DiResta notes, the widespread use of numerous applications and platforms illustrates "the fluid, evolving, and innovative tactical approach the IRA leveraged to interfere in US politics and culture."[250]

---

[246] **(U)** *Ibid.*
[247] **(U)** Blake Lawit, General Counsel, LinkedIn, *Letter to SSCI,* December 21, 2018.
[248] **(U)** Jonathan Landay and Warren Strobel, "Exclusive: U.S. Accuses China of "Super Aggressive" Spy Campaign on LinkedIn," *Reuters,* August 31, 2018.
[249] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.
[250] **(U)** *Ibid.*

VIII. (U) OTHER RUSSIAN SOCIAL MEDIA INFORMATION WARFARE EFFORTS

A. (U) Main Intelligence Directorate (GRU)

(U) Other Russian government-funded and -directed entities, particularly the Russian intelligence services, also conducted social media efforts directed at the 2016 U.S. election. The Russian GRU conducted a wide variety of activities on social media. In January 2018 written responses to Committee inquiries, Facebook confirmed the presence of activity attributed to the GRU (also known as Fancy Bear or APT28) on its platform: "We have also tracked activity from a cluster of accounts we have assessed to belong to a group, APT28, that the U.S. government has publicly linked to Russian military intelligence services and the 'DCLeaks' organization."[251]

(U) Much of the activity related to APT28 found by Facebook in 2016 appeared to Facebook security experts as consistent with more typical offensive cyber activities, generally attributed to foreign intelligence services, including the targeting and attempted hacking of "employees of major U.S. political campaigns." However, Facebook later detected the APT28 group's engagement in what they described as "a new kind of behavior" later in the summer of 2016. Facebook uncovered GRU attempts to engage in influence activities, namely, "the creation of fake personas that were then used to seed stolen information to journalists." As Facebook notes, "These fake personas were organized under the banner of an organization that called itself 'DCLeaks.'"[252]

(U) The GRU's direct role in the 2016 information warfare campaign was publicly exposed in yet another indictment obtained in July 2018 by the Special Counsel's Office. This indictment against the GRU ("the GRU indictment") outlined very specific details about the GRU's online influence operations.

(U) The GRU indictment charged a number of GRU operatives, including Aleksandr Vladimirovich Osadchuk, a colonel in the Russian military and the commanding officer of the GRU's unit 74455. The Special Counsel's Office described Unit 74455's role in the GRU's influence operation: "Unit 74455 assisted in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU."

(U) The public accounting from the Special Counsel's Office also reveals the cross-platform character of these information operations, which involved several of the social media companies, including Facebook and Twitter.[253]

---

[251] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf

[252] **(U)** *Ibid.*

[253] **(U)** Indictment, *United States v. Viktor Borisovich Netyksho, et al.*, Case 1:18-cr-00215-ABJ (D.D.C. July 13, 2018).

(U) On *or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name "Alice Donovan." In addition to the DCLeaks Facebook page, the Conspirators used other social media accounts in the names of fictitious U.S. persons such as "Jason Scott" and "Richard Gingrey" to promote the DCLeaks website.*[254]

(U) *On or about June 8, 2016, the Conspirators created the Twitter account @dcleaks_. The Conspirators operated the @dcleaks_ Twitter account from the same computer used for other efforts to interfere with the 2016 U.S. presidential election. For example, the Conspirators used the same computer to operate the Twitter account @BaltimoreIsWhr, through which they encouraged U.S. audiences to "[j]oin our flash mob" opposing Clinton and to post images with the hashtag #BlacksAgainstHillary.*[255]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[254] **(U)** *Ibid.*
[255] **(U)** *Ibid.*

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

256 [redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

- [redacted]

- [redacted]

[redacted]

(U) According to FBI:

[redacted]

[redacted]

[redacted]

(U) A 2017 analysis by cybersecurity company FireEye outlined additional personas assessed to be associated with Kremlin-linked organizations. From FireEye's report: "We assess, with varying respective degrees of confidence, that Russian state-sponsored actors leveraged at least six false 'hacktivist' personas over the course of 2016 to conduct a series of information operations designed to further Russian political interests."[258] Personas attributed to Russian state sponsors included Guccifer 2.0, DCLeaks, @anpoland (Anonymous Poland), Fancy Bears' Hack Team, @pravsector (Pravvy Sektor), and Bozkurt Hackers.[259]

(U) According to the 2017 analysis by FireEye: "Personas engaged in highly organized, systematized, and in some cases semi-automated social media dissemination campaigns to promote leaks and associated political narratives to media outlets and other influencers, in order to generate mainstream coverage and public attention." The activities included "cadres of Twitter accounts repetitively publishing identical tweets promoting threat activity. [The accounts were] [d]esigned to further spread awareness of incidents and boost the credibility of the personas by creating a grassroots impression that more genuine Twitter users are talking about incidents than is accurate."[260]

(U) Even as late as the fall of 2018, Facebook continued to find activity attributed to the GRU. In August 2018, Facebook announced additional actions against "Pages, groups and accounts that can be linked to sources the US government has previously identified as Russian military intelligence services."[261] As detailed by this enforcement of Facebook's terms of service, Russian-backed influence operations did not stop after the 2016 U.S. election.

---

[257] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.
[258] **(U)** FireEye, "Anatomy of Russia's 2016 Influence Operations: Hacks, leaks, and the manipulation of political opinion," FireEye, Inc., October 2017.
[259] **(U)** The *New York Times* reported in September 2017 about activity sponsored by Anonymous Poland Twitter accounts that were involved in spreading political disinformation during the 2016 U.S. election. Their article noted "last October [2016], hundreds of Anonymous Poland Twitter accounts posted a forged letter on the stationery of the conservative Bradley Foundation . . . purporting to show that it had donated $150 million to the Clinton campaign. The foundation denied any such contribution, which would have been illegal and . . . highly unlikely."
[260] **(U)** FireEye, "Anatomy of Russia's 2016 Influence Operations: Hacks, leaks, and the manipulation of political opinion," FireEye, Inc., October 2017.
[261] **(U)** Facebook Newsroom, "Taking Down More Coordinated Inauthentic Behavior," Facebook, August 21, 2018, https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/.

B. [redacted]

[redacted]

- [redacted]

- [redacted]

---

[262] [redacted]

[263] **(U)** *Ibid.*

[264] **(U)** *Ibid.*

[265] [redacted]

[266] **(U)** *Ibid.*

[267] **(U)** *Ibid.*

[redacted]

- [redacted]

- [redacted]

C. (U) Other Russian Government Activities

(U) In fall 2016, an FBI contractor analyzed a pro-Russian network of 13 Twitter accounts. The account @TeamTrumpRussia was the central node in this network. According to FBI:

> **(U)** *@TeamTrumpRussia and the other 12 accounts had a total of 1,504,511 followers at the time the contractor collected its data (17 to 19 October 2016). Four of the 13 accounts had a reciprocal relationship with Sergey Nalobin, an employee of Russia's Ministry of Foreign Affairs (MFA), whose Twitter profile states he is responsible for "digital diplomacy and social media." In August 2015, the United Kingdom refused to extend Nalobin's visa because of his involvement with a UK political group called "Conservative Friends of Russia," according to open source reporting.*
>
> **(U)** *The FBI contractor found over 70 percent of the network's Tweets contained links to Websites "outside of the mainstream US press, and are known to be*

[268] [redacted]
[269] [redacted]
[270] **(U)** *Ibid.*
[271] [redacted]
[272] **(U)** *Ibid.*

highly supportive of the Trump campaign. Of those sites, a number are also known to overtly draw content from Russian disinformation sites or are suspected of more covert connections to the Kremlin."

[redacted] *A second report produced by the contractor examined the network's efforts to promote allegations of voter fraud in advance of the election,* [redacted]

[redacted]

IX. (U) U.S. GOVERNMENT RESPONSE

(U) Throughout the 2016 U.S. presidential election campaign period, the IRA was a largely obscure entity operating far from America's borders inside a stand-alone building in St. Petersburg, Russia. Despite the fact that the IRA began planning and implementing its electoral interference as early as 2014, its existence and activities were not well known to the wider American public and the U.S. Government until well after the election had passed. Even the January 6, 2017 Intelligence Community Assessment, authored as the Intelligence Community's comprehensive account of Russia's attack on the U.S. election, made no more than a passing reference to the cadre of professional trolls housed in the IRA.[275] In early September 2017, Facebook—under significant pressure from this Committee and the broader United States Congress—disclosed a collection of accounts linked to the IRA, beginning to bring the scope of

[273] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.

[274] [redacted]

[275] [redacted]

the IRA's electoral activities into focus.[276] The criminal nature of the IRA's interference crystallized with the Special Counsel's public indictment in February 2018.[277]

(U) Some of the starkest early insights into IRA activities for western audiences were reported by *The Guardian*'s Shaun Walker in his April 2015 report, "Salutin' Putin," and by Adrian Chen in *The New York Times Magazine* investigative report on the IRA, "The Agency."[278] These investigative reports take on new significance in light of the Committee's work.

(U) The U.S. Intelligence Community's ability to identify and combat foreign influence operations carried out via social media channels has improved since the 2016 U.S. presidential election. Communication and information sharing between government agencies and the social media companies has been a particular point of emphasis, and the Committee strongly supports these efforts. Characterizing the company's present relationship with Federal law enforcement, Twitter representatives have informed the Committee, "We now have well-established relationships with law enforcement agencies active in this arena, including the Federal Bureau of Investigation Foreign Influence Task Force and the U.S. Department of Homeland Security's Election Security Task Force."[279] Facebook has made similar representations to the Committee:

> *After the election, when the public discussion of 'fake news' rapidly accelerated, we continued to investigate and learn more about the new threat of using fake accounts to amplify divisive material and deceptively influence civic discourse. We shared what we learned with government officials and others in the tech industry. Since then, we also have been coordinating with the FBI's Counterintelligence Division and the DOJ's National Security Division. We are also actively engaged with the Department of Homeland Security, the FBI's Foreign Influence Task Force, and Secretaries of State across the US on our efforts to detect and stop information operations, including those that target elections.*[280]

(U) This progress notwithstanding, it is important to memorialize the state of information sharing between law enforcement and the social media companies in fall 2016. The FBI was examining social media content for its potential as a means of effectuating foreign influence operations in 2016, but mostly through contractors:

---

[276] **(U)** Alex Stamos, Facebook, "An Update on Information Operations on Facebook," September 6, 2017: https://newsroom.fb.com/news/2017/09/information-operations-update/.

[277] **(U)** The first publicly available insight into the IRA, however, came several years prior as a result of the efforts of a small number of diligent and prescient reporters. By 2015, Russian reporters, including Andrei Soshnikov who went undercover as a troll in the IRA in 2013, had begun to expose the inner workings of the IRA.

[278] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015; Adrian Chen, "The Agency," *The New York Times Magazine*, June 2, 2015.

[279] **(U)** Sean Edgett, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, January 25, 2019.

[280] **(U)** Facebook, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, February 26, 2019

(U) *In October 2016, the Counterintelligence Division tasked a contractor to identify Russian influence activity on Twitter. The FBI contractor collected and analyzed a sample of Twitter activity conducted by an overtly pro-Russian network of 13 Twitter accounts and their followers, including automated accounts, which promoted US election-related news and leaked Democratic party emails published by WikiLeaks.*[281]

(U) The apparently outsourced nature of this work is troubling: it suggests FBI either lacked resources or viewed work in this vein as not warranting more institutionalized consideration. None of the resulting analysis or even notice of the underlying activity appears to have been communicated to the social media company in question prior to the election. Twitter's General Counsel told the Committee in January 2019: "To the best of our knowledge, Twitter received no information from the U.S. government in advance of the 2016 election about state sponsored information operations."[282]

(U) Facebook, however, had more robust information exchange with law enforcement in 2016: "In several instances before the 2016 U.S. election, our threat intelligence team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials, and they subsequently shared useful feedback with us."[283] Still, it was incumbent on Facebook to initiate the dialogue with law enforcement, and the exchange of information was predicated on Facebook bringing foreign influence activity directed at Americans to the attention of the FBI.

[redacted]

[redacted] Reflecting on the U.S. Government's handling of social media in the context of Russia's influence operations, former Deputy National Security Advisor for Strategic Communications Ben Rhodes commented [redacted]

---

[281] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.
[282] **(U)** Sean Edgett, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, January 25, 2019.
[283] **(U)** Facebook, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, February 26, 2019
[284] **(U[redacted])** Committee transcript of September 15, 2017 interview of [redacted] CIA.

[redacted] Commenting on the [redacted] Former Homeland Security Advisor Lisa Monaco offered a [redacted]

[redacted]

(U) Further increasing this challenge, detecting foreign influence operations on social media becomes more difficult as enabling technologies improve. In addition to the growing number of actors engaged in social media-facilitated, online manipulation efforts, the technology that aids in developing more realistic and convincing propaganda material also continues to advance.

(U) The ongoing development of artificial intelligence and improvements to false video and image "Deepfake" techniques are making it more difficult to spot fake content, manipulated videos, and forged recordings online. "Deepfakes" entail using artificial intelligence-based technology to create or alter video content so that it appears to present something that did not actually occur. Although these capabilities are relatively nascent, they are being perfected at a pace that eclipses the effort to create the technology for detecting and mitigating fraudulent media content.

(U) Advanced micro-targeting in the commercial sector is also rapidly becoming more effective. Propagandists will be able to continue to utilize increasingly advanced off-the-shelf capabilities to target specific individuals with highly targeted messaging campaigns.

---

[285] **(U)** SSCI Transcript of the Interview with Benjamin J. Rhodes, Former Deputy National Security Adviser for Strategic Communications, July 25, 2017.
[286] **(U)** *Ibid.*
[287] **(U)** SSCI transcript of the Closed Hearing on White House Awareness of and Response to Russian Active Measures, July 17, 2018.
[288] **(U)** SSCI Transcript of the Interview with John Carlin, Former Assistant Attorney General for National Security, September 25, 2017.

(U) Automation is also getting better. Bots—already advanced in sophistication relative to predecessor generations—are becoming harder and harder to detect. Researchers, including Emilio Ferrara and his team from the University of Southern California and the University of Indiana, have studied the increasing sophistication of automated accounts. Their research suggests a detection "arms race," between the purveyors of automated activity and those intent on its reliable identification, similar to the fight against the indiscriminate dissemination of commercial content to vast unsoliciting audiences, or "spam," in the past.[289]

(U) In addition, as the larger social media platforms begin to increase their detection capabilities, disinformation tactics have begun to shift to accommodate those changes. Influence operatives have begun to move away from targeting Facebook and Twitter newsfeeds, transitioning to messaging platforms like WhatsApp, Telegram, and WeChat. These direct interactions are much harder to detect and if these tactics are scaled, they could have a significant effect on target audiences.

(U) The evolution and proliferation of the core influence techniques used by the IRA could jeopardize facets of American society that have yet to be attacked by influence operatives. The same bots, trolls, click-farms, fake pages and groups, advertisements, and algorithm-gaming the IRA used to conduct an information warfare campaign can be repurposed to execute financial fraud, stock-pumping schemes, digital advertising manipulation, industrialized marketing of counterfeit prescription drugs, and scaled deceptions that spread malware.

[redacted] Facebook CEO Sheryl Sandberg testified to the Committee in 2018 that, "Our focus is on inauthenticity, so if something is inauthentic, whether it's trying to influence domestically or trying to influence on a foreign basis—and actually a lot more of the activity is domestic—we take it down."[291] But as the IRA's approach suggests, the current constructs for removing influence operation content from social media are being surpassed by foreign influence operatives, who adapt their tactics to either make their inauthenticity indiscernible, their automated propagation too rapid to control, or their operations compliant with terms of service.

(U) An October 2018 report provided to the Committee by social media analytics firm Graphika indicates that Russian disinformation efforts may be focused on gathering information and data points in support of an active measures campaign targeted at the 2020 U.S. presidential

---

[289] **(U)** Emilio Ferrara, et al., "The Rise of Social Bots," *Communications of the ACM*, July 2016, Volume 59, Number 7, 96-104, https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext#R22.

[290] [redacted]

[291] **(U)** Sheryl Sandberg, Hearing before the Senate Select Committee on Intelligence, September 5, 2018, available at https://www.intelligence.senate.gov/hearings/open.

election. The USA Really website and its affiliated social media channels, which have been linked to the IRA on the basis of technical findings, have "engaged in a number of campaigns seemingly focused on gathering personal information (emails, phone numbers, and bank details) of US-based audiences sympathetic to Russian disinformation topics."[292]

X. (U) THE COMMITTEE'S REVIEW OF RUSSIA'S USE OF SOCIAL MEDIA

(U) Throughout 2017, 2018, and 2019, in addition to its review of classified information on the topic, the Committee worked to elevate public awareness of the threat posed by Russia online, an effort that included applying pressure on social media companies to more fully examine their platforms for suspected Russian government activities.

(U) On March 30, 2017, the Committee held a public hearing for the purpose of discussing Russian malign influence efforts. The hearing, entitled "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," included testimony from a number of expert witnesses who provided insights into the mechanics of Russian influence operations and warned that Russian social media manipulation "has not stopped since the election in November and continues fomenting chaos amongst the American populace."[293] Committee Members joined witnesses in calling on social media companies to do more to uncover the Russian active measures activities occurring on their platforms. In the wake of the hearing, the Committee publicly and privately pressed social media companies to release more information about the activity of Russian actors on social media in the lead-up to the 2016 election.

(U) On April 27, 2017, Facebook released a white paper detailing an array of malicious information operations by organized actors on the Facebook social media platform.[294] Though the paper implicitly attributed the operations to Russian intelligence actors, the company had yet to uncover the substantial operational activity of the IRA.[295] Finally, in late summer 2017, Facebook notified the Committee of its findings from an internal information security investigation which uncovered 470 accounts, groups, and pages linked to the IRA.[296]

---

[292] **(U)** Graphika Strategic Assessment, *USA Really Shows a New Face of Russian Disinformation Efforts Against the US*, October 10, 2018.

[293] **(U)** Clint Watts, Written Testimony, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[294] **(U)** Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook," Facebook Newsroom, April 27, 2017, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

[295] **(U)** The Facebook white paper specifically stated that Facebook was not in a position to make "definitive attribution" to the actors sponsoring this activity. However, it was willing to publicly say that the data it uncovered "does not contradict the attribution provided by the U.S. Director of National Intelligence in the report dated January 6, 2017." This is a clear reference to Russian-linked activity. Alex Stamos, one of the authors of the white paper, also made clear to SSCI staff in a briefing around that time that indicators pointed to Russian-linked intelligence activity.

[296] **(U)** Facebook briefed Committee staff on its findings on September 6, 2017, and publicized those same findings later that day.

(U) The subsequent September 2017 release of IRA-linked account information by Facebook publicly confirmed the existence of IRA-purchased advertisements. This precipitated audits at Twitter, Google, YouTube, Reddit, and other social media companies, which uncovered additional accounts and activity originating with the IRA. As more and more information became public, the wide-ranging and cross-platform nature of the attack emerged. The Committee made formal requests to multiple social media companies for any data associated with these operations, in order to better assess Russia's tactics and objectives. On the basis of negotiations with the Committee, several companies—including Facebook, Twitter, and Google—furnished varying quantities of data not previously released.

(U) Beginning with an initial delivery of metadata and content in late 2017, Facebook, Twitter, and Google provided the Committee with information relating to a number of IRA-affiliated social media accounts, including advertisements purchased in connection with those accounts, consisting of:

- Metadata and content associated with 81 Facebook Pages, including approximately 61,500 unique Facebook organic posts and 3,393 paid advertisements;
- Similar information from nearly 116,000 Instagram posts across 133 Instagram accounts;
- Metadata and content of approximately 10.4 million tweets across 3,841 Twitter accounts, as well as unique account information; and,
- Approximately 1,100 YouTube videos (43 hours of video) across 17 account channels.

(U) Each of these accounts and their associated activities were determined to be connected to the IRA by the social media companies themselves, based on the companies' internal investigations.[297] This cooperation by the social media companies secured for the Committee a significant and unique dataset on which to base further study into IRA activities. Much of the analysis in this report derives from that initial dataset.[298] The datasets provided to the Committee demonstrate the IRA's tactics and capabilities, and add depth to the public's understanding of how the IRA conducted its information warfare campaign against the United States in 2016.

(U) In order to thoroughly examine this sizeable aggregation of technical data, the Committee sought assistance from the TAG. At the Committee's request, the two TAG working

[297] **(U)** The Committee has not attempted to make an independent determination as to the accuracy of the social media companies' internal investigations or the true provenance of the accounts themselves, though the Committee does believe that the data provided is almost certainly not the entirety of the IRA's activity on these platforms. Subsequent reporting and additional research from outside analysts have corroborated much of the original attribution from the companies.

[298] **(U)** Twitter has since published its entire dataset on IRA-linked activity. On October 17, 2018, Twitter publicly released all the accounts and related content it has identified so far as associated with the activities of the IRA, dating back to 2009.

groups each conducted an independent, expert analysis of the social media company-provided dataset. Combining this dataset with the TAG's own internal research and data analytic capabilities, the TAG working groups studied U.S. social media platforms for indications of additional and undiscovered Russian foreign influence activity. Ultimately, the three TAG working group leads provided their findings and analysis to the Committee in a series of presentations that included staff briefings, a closed Member briefing, and a full Committee public hearing held on August 1, 2018.

(U) The TAG working groups each published their findings in two public reports that were released on December 17, 2018. The efforts of the TAG working groups, and the team leads specifically, resulted in two valuable publications that have significantly informed the Committee's understanding of Russia's social media-predicated attack against our democracy. The Committee supports the general findings of the TAG working groups, and notes that much of this Volume's analysis is derived from their work. The two reports are attached as addendums to this Volume.

XI. (U) RECOMMENDATIONS

(U) This challenge requires an integrated approach that brings together the public and private sectors. This approach must be rooted in protecting democratic values, including freedom of speech and the right to privacy. The Federal government, civil society, and the private sector, including social media and technology companies, each have an important role to play in deterring and defending against foreign influence operations that target the United States.

A. (U) Industry Measures

(U) The Committee recommends that social media companies work to facilitate greater information sharing between the public and private sector, and among the social companies themselves about malicious activity and platform vulnerabilities that are exploited to spread disinformation. Formalized mechanisms for collaboration that facilitate content sharing among the social media platforms in order to defend against foreign disinformation, as occurred with violent extremist content online, should be fostered. As researchers have concluded: "Many disinformation campaigns and cyber threats do not just manipulate one platform; the information moves across various platforms or a cyber-attack threatens multiple companies' network security and data integrity. There must be greater cooperation within the tech sector and between the tech sector and other stakeholders to address these issues."[299] The Committee agrees.

(U) This should not be a difficult step. Models for cooperation already exist and can be developed further:

[299] **(U)** *Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation*, Stern Center for Business and Human Rights, New York University, November 3, 2017, http://www.stern.nyu.edu/experience-stern/faculty-research/harmful-content-role-internet-platform- companies-fighting-terrorist-incitement-and-politically.

- **(U)** Google, Facebook, Twitter, and Microsoft already maintain a common database of digital fingerprints identifying violent extremist videos. These four companies also participate in a Cyberhate Problem-Solving Lab run by the Anti-Defamation League's Center for Technology and Society.

- **(U)** Dozens of tech companies participate in the Global Network Initiative, a tech policy forum devoted to protecting digital rights globally.

- **(U)** Other examples include the Global Internet Forum to Counter Terrorism, whose goal is to substantially disrupt terrorists' ability to disseminate violent extremist propaganda, and glorify real-world acts of violence; and the National Cyber Forensics and Training Alliance, a nonprofit partnership between industry, government, and academia that enables cooperation to disrupt cyber-crime.

- **(U)** Two models from the world of financial intelligence are the UK's Joint Money Laundering Intelligence Taskforce and the United States' Financial Crimes Enforcement Exchange.

(U) At the urging of the Committee, social media companies have begun to share indicators, albeit on an ad hoc basis.

(U) The Committee further recommends that social media companies provide users with:

- **(U)** Greater transparency about activity occurring on their platforms, including disclosure of automated accounts (i.e., bots);

- **(U)** Greater context for users about why they see certain content;

- **(U)** The locational origin of content; and,

- **(U)** Complete and timely public exposure of malign information operations.

(U) Social media platforms are not consistent in proactively, clearly, and conspicuously notifying users that they have been exposed to these efforts, leaving those who have been exposed to the false information or accounts without the knowledge they need to better evaluate future social media content that they encounter. Notifications to individual users should be clearly stated, device neutral, and provide users all the information necessary to understanding the malicious nature of the social media content or accounts they were exposed to.

(U) Finally, the analytic and computational capabilities of outside researchers should be put to greater use by the social media companies. Although social media companies have released some data about the manipulation of their platforms by foreign actors, the Committee recommends that social media companies be more open to facilitating third-party research

designed to assist them in defending their platforms from disinformation campaigns. The results of collaboration with outside researchers should be shared with users who have been exposed to disinformation.

B. (U) Congressional Measures

(U) The Committee recommends that Congress consider ways to facilitate productive coordination and cooperation between U.S. social media companies and the pertinent government agencies and departments, with respect to curtailing foreign influence operations that target Americans—to include examining laws that may impede that coordination and cooperation. Information sharing between the social media companies and law enforcement must improve, and in both directions. Data must be shared more quickly and in a more useful manner. This will improve the ability of social media companies to quickly identify and disclose malign foreign influence operations to the appropriate authorities, and it will improve the ability of law enforcement agencies to respond in a timely manner.

(U) Informal channels of communication may not be sufficient to accomplish this goal. As part of its examination, Congress must assess whether formalized information sharing between law enforcement and social media companies is useful and appropriate. Certain statutory models already exist, such as U.S. Code, Title 18, Section 2258A (Reporting requirements of providers). That section requires social media companies to report any apparent violations of laws relating to child sexual exploitation to the National Center for Missing and Exploited Children (NCMEC). NCMEC is a private, non-profit entity that serves a statutorily authorized clearinghouse role: it receives the providers' reports, assesses the reports for criminality and threats to children, and refers them to the appropriate law enforcement authorities for action. Formalizing a relationship between social media companies and the government does present some legal considerations,[300] but these should not be prohibitive.

(U) Further, the Committee recommends that Congress examine legislative approaches to ensuring Americans know the sources of online political advertisements. The Federal Election Campaign Act of 1971 requires political advertisements on television, radio and satellite to disclose the sponsor of the advertisement. The same requirements should apply online. This will also help to ensure that the IRA or any similarly situated actors cannot use paid advertisements for purposes of foreign interference.

(U) Finally, Congress should continue to examine the full panoply of issues surrounding social media, particularly those items that may have some impact on the ability of users to masquerade as others and provide inauthentic content. Issues such as privacy rules, identity

[300] **(U)** For example, courts have considered whether NCMEC and providers should be considered state actors and therefore subject to Constitutional requirements such as the Fourth Amendment when identifying and sharing child exploitation material with law enforcement. *See, e.g.*, *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018) (holding that provider acted in a private capacity when identifying and reporting child exploitation images to NCMEC); *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) (holding that NCMEC was a state actor when reviewing and reporting child exploitation material to law enforcement).

validation, transparency in how data is collected and used, and monitoring for inauthentic or malign content, among others, deserve continued examination. In addition, Congress should monitor the extent to which social media companies provide users with the information laid out in section A and, if necessary, take remedial steps.

C. (U) Executive Branch Measures

(U) The Committee recommends that the Executive Branch should, in the run up to the 2020 election, reinforce with the public the danger of attempted foreign interference in the 2020 election.

(U) Addressing the challenge of disinformation in the long-term will ultimately need to be tackled by an informed and discerning population of citizens who are both alert to the threat and armed with the critical thinking skills necessary to protect against malicious influence. A public initiative—propelled by federal funding but led in large part by state and local education institutions—focused on building media literacy from an early age would help build long-term resilience to foreign manipulation of our democracy. Such an effort could benefit from the resources and knowledge of private sector technology companies.

(U) Additionally, and in concert with initiatives that heighten public awareness about disinformation, media organizations should establish guidelines for using social media accounts as sources, to guard against quoting falsified accounts or state-sponsored disinformation.

(U) The Committee further recommends that the Executive Branch stand up an interagency task force to continually monitor and assess foreign country's use of social media platforms for democratic interference. The task force should periodically advise the public and Congress on its findings and issue annual reports providing recommendations to key actors, including executive branch departments and agencies, industry, and civil society. The task force should also develop a deterrence framework to inform U.S. Government responses to foreign influence efforts using social media.

(U) The Committee further recommends that the Executive Branch develop a clear plan for notifying candidates, parties, or others associated with elections when those individuals or groups have been the victim of a foreign country's use of social media platforms to interfere in an election. The plan should provide standards for deciding who to notify and when, and should clearly delineate which agencies are responsible for making the notifications and to whom.

D. (U) Other Measures

(U) The Committee recommends that candidates, campaigns, surrogates for campaigns, and other public figures engaged in political discourse on social media be judicious in scrutinizing the sources of information that they choose to share or promote online. Such public figures, precisely because of the reach of their networks, are valuable targets for adversaries, and can quickly be co-opted into inadvertently promoting a foreign influence operation.

(U) Amplification of foreign content, intentional or otherwise, is celebrated by those like the IRA, who wish to enflame our differences in order to advance their own interests. The Committee recommends that all Americans, and particularly those with a public platform, take on the responsibility of doing due diligence in their use of social media, so as to not give greater reach to those who seek to do our country harm.

(U) The Committee recommends the implementation of a Public Service Announcement (PSA) campaign, potentially by the social media industry or by government actors, that promotes informed social media behavior and raises awareness about various types of foreign influence and interference activity that is targeting American citizens, businesses, and institutions. Foreign influence campaigns that target social media users in the United States should receive similar attention to the dangers of smoking and the environmental risks of pollution. Broader exposure of specific foreign government linkages to social media content and influence activities would handicap the effectiveness of information operations.

[redacted]

XII. (U) Additional Views of Senator Wyden

(U) If American democracy is going to withstand the onslaught of foreign government influence campaigns targeting U.S. elections, our government must address the problem of targeted ads and other content tailored to consumers' demographic and political profiles. Targeted influence campaigns can weaponize personal information about Americans, not just to manipulate how, or whether they vote, but to identify and use real individuals to amplify content and influence like-minded followers. Targeted influence campaigns are far more effective and cost-efficient than blanket dissemination of propaganda. They are also more deceptive and substantially harder to identify and expose.

(U) While the Committee's description of Russia's 2016 influence campaign is deeply troubling, even more sophisticated and effective options are available to adversaries who buy, steal, or otherwise obtain information about the Americans they are seeking to influence. This threat is increased due to the availability of ad micro-targeting services offered by social media and online advertising companies, particularly those that deliver ads to specific Americans based on a list of email addresses or telephone numbers provided by an advertiser. Such ad targeting systems are highly prone to abuse when coupled with private information about Americans, which is widely available because of weak corporate data security and privacy practices, the absence of strong privacy laws, and the booming market for commercial data brokers, whose practices are largely unregulated. Each of these problems demands an effective response.

(U) The Committee report states that, in 2016, IRA operators did not take advantage of all of Facebook's targeting capabilities, including "Custom Audiences," which would have allowed the Russians to use outside data and contact information to conduct "advanced micro-targeting."[1] The danger posed by these services is magnified by the ease with which personal data can be purchased or stolen by a foreign adversary with advanced cyber capabilities. Indeed, as the Department of Justice's indictment against the IRA revealed, the IRA used stolen identities of real Americans to create accounts and post content, purchase advertising on social media sites and finance their influence activities through Pay Pal.[2]

(U) In the wake of the 2016 influence campaign by Russia, the social media companies announced transparency measures that allow the recipients of targeted ads to understand how they were selected to see the ads. However, these transparency measures only apply when the tech companies are doing the targeting on behalf of the advertiser, for example when an advertiser asks Facebook to deliver its ads to a particular age and gender demographic. The companies' ad transparency systems do not apply to services like Custom Audiences through which the platform merely serves as a messenger for ads directed according to a list of targets obtained by the malign influencer from a data broker or a hacked database. I have already publicly called on the social media platforms to voluntarily suspend the use of Custom Audiences and other micro-targeting services for political and issue ads, and I repeat that call

[1] (U) Facebook has acknowledged that the IRA used custom audiences based on user engagement with certain IRA pages. *See* Responses by Facebook to Questions for the Record from Senator Wyden from hearing on September 5, 2018, submitted October 26, 2018, p. 45.

[2] (U) Indictment, *United States of America v. Internet Research Agency et al.*, Case 1:18-cr-00032-DLF (D.D.C. February 16, 2018).

[redacted]

[redacted]

here.[3] Until Facebook, Google, and Twitter have developed effective defenses to ensure that their ad micro-targeting systems cannot be exploited by foreign governments to influence American elections, these companies must put the integrity of American democracy over their profits.

(U) At the Committee's September 5, 2018, hearing, I asked Facebook's Chief Operating Officer Sheryl Sandberg and Twitter's Chief Executive Officer Jack Dorsey whether increased protections and controls to defend personal privacy should be a national security priority. Both witnesses answered in the affirmative. Weak data privacy policies increase the ability of foreign adversaries to micro-target Americans for purposes of election interference. Facebook's total failure to prevent Cambridge Analytica and Aleksandr Kogan from obtaining sensitive personal data about Facebook users, as well as Facebook's troubling data-sharing partnerships with Chinese smart phone manufacturers, demonstrate clear gaps in federal data privacy laws and highlight obvious weaknesses that could be exploited in future influence campaigns.[4]

(U) Broad, effective data security and privacy policies, implemented across the platforms and enforced by a tough, competent government regulator, are necessary to prevent the loss of consumers' data and the abuse of that data in election influence campaigns. Congress should pass legislation that addresses this concern in three respects. First, the Federal Trade Commission must be given the power to set baseline data security and privacy rules for companies that store or share Americans' data, as well as the authority and resources to fine companies that violate those rules. Second, companies should be obligated to disclose how consumer information is collected and shared and provide consumers the names of every individual or institution with whom their data has been shared. Third, consumers must be given the ability to easily opt out of commercial data sharing.

(U) Companies that hold private information on Americans also must do far more to protect that information from hacking. That includes telecommunications companies that hold information about customers' communications, web browsing, app usage and location. Too much of this information is held for too long, increasing the risk that it will be hacked. Besides strengthening their cyber security practices, companies can take steps to delete consumer information as soon as it is not absolutely necessary for business purposes.

(U) Increased transparency is another critical priority if the United States is to defend itself against foreign election influence campaigns. A clear lesson from 2016 is that the U.S. public needs information about influence campaigns prior to the election itself. That includes information about U.S. adversaries' attempts to undermine some candidates while assisting others. In 2016, the specific intent of the Russians was not made public during the election. Intelligence related to Russian intent was not even made available to the full Committee until after the election, at which point I and other members called for its declassification. And it was not until the publication of the Intelligence Community Assessment in January 2017 that the public was finally provided this information.

---

[3] **(U)** Donie O'Sullivan, "Senator calls on Facebook and Google to ban political ad targeting," *CNN*, August 14, 2019.

[4] **(U)** *See* Responses by Facebook to Questions for the Record from Senator Wyden from hearing on September 5, 2018, submitted October 26, 2018, pp. 46-55.

[redacted]

[redacted]

[redacted][5] Between now and the 2020 election, the Intelligence Community must find ways to keep the U.S. public informed not only of individual influence operations, but the Community's assessment of the goals and intent of Russia and other foreign adversaries.

[5] [redacted] National Intelligence Council, Sense of the Community Memorandum, "[redacted]," September 13, 2019.

[redacted]