Report On The Investigation Into Russian Interference In The 2016 Presidential Election

Volume I of II

Special Counsel Robert S. Mueller, III

Submitted Pursuant to 28 C.F.R. §600.8(c)

Washington, D.C.

March 2019

Open Source Edition
https://github.com/iandennismiller/mueller-report

Table of Contents - Volume 1

TABLE OF CONTENTS - VOLUME 1

Introduction to Volume I

This report is submitted to the Attorney General pursuant to 28 C.F.R. §600.8(c), which states that, "[a]t the conclusion of the Special Counsel's work, he ... shall provide the Attorney General a confidential report explaining the prosecution or declination decisions [the Special Counsel] reached."

The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion. Evidence of Russian government operations began to surface in mid-2016. In June, the Democratic National Committee and its cyber response team publicly announced that Russian hackers had compromised its computer network. Releases of hacked materials-hacks that public reporting soon attributed to the Russian government-began that same month. Additional releases followed in July through the organization WikiLeaks, with further releases in October and November.

In late July 2016, soon after WikiLeaks's first release of stolen documents, a foreign government contacted the FBI about a May 2016 encounter with Trump Campaign foreign policy advisor George Papadopoulos. Papadopoulos had suggested to a representative of that foreign government that the Trump Campaign had received indications from the Russian government that it could assist the Campaign through the anonymous release of information damaging to Democratic presidential candidate Hillary Clinton. That information prompted the FBI on July 31, 2016, to open an investigation into whether individuals associated with the Trump Campaign were coordinating with the Russian government in its interference activities.

That fall, two federal agencies jointly announced that the Russian government "directed recent compromises of e-mails from US persons and institutions, including US political organizations," and, "[t]hese thefts and disclosures are intended to interfere with the US election process." After the election, in late December 2016, the United States imposed sanctions on Russia for having interfered in the election. By early 2017, several congressional committees were examining Russia's interference in the election.

Within the Executive Branch, these investigatory efforts ultimately led to the May 2017 appointment of Special Counsel Robert S. Mueller, III. The order appointing the Special Counsel authorized him to investigate "the Russian government's efforts to interfere in the 2016 presidential election," including any links or coordination between the Russian government and individuals associated with the Trump Campaign.

As set forth in detail in this report, the Special Counsel's investigation

established that Russia interfere in the 2016 presidential election principally through two operations. First, a Russian entity carried out a social media campaign that favored presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton. Second, a Russian intelligence service conducted computer-intrusion operations against entities, employees, and volunteers working on the Clinton Campaign and then released stolen documents. The investigation also identified numerous links between the Russian government and the Trump Campaign. Although the investigation established that the Russian government perceived it would benefit from a Trump presidency and worked to secure that outcome, and that the Campaign expected it would benefit electorally from information stolen and released through Russian efforts, the investigation did not establish that members of the Trump Campaign conspired or coordinated with the Russian government in its election interference activities.

Below we describe the evidentiary considerations underpinning statements about the results of our investigation and the Special Counsel's charging decisions, and we then provide an overview of the two volumes of our report.

The report describes actions and events that the Special Counsel's Office found to be supported by the evidence collected in our investigation. In some instances, the report points out the absence of evidence or conflicts in the evidence about a particular fact or event. In other instances, when substantial, credible evidence enabled the Office to reach a conclusion with confidence, the report states that the investigation established that certain actions or events occurred. A statement that the investigation did not establish particular facts does not mean there was no evidence of those facts.

In evaluating whether evidence about collective action of multiple individuals constituted a crime, we applied the framework of conspiracy law, not the concept of "collusion." In so doing, the Office recognized that the word "collud[e]" was used in communications with the Acting Attorney General confirming certain aspects of the investigation's scope and that the term has frequently been invoked in public reporting about the investigation. But collusion is not a specific offense or theory of liability found in the United States Code, nor is it a term of art in federal criminal law. For those reasons, the Office's focus in analyzing questions of joint criminal liability was on conspiracy as defined in federal law. In connection with that analysis, we addressed the factual question whether members of the Trump Campaign" coordinat[ed]" - a term that appears in the appointment order - with

Russian election interference activities. Like collusion, "coordination" does not have a settled definition in federal criminal law. We understood coordination to require an agreement - tacit or express - between the Trump Campaign and the Russian government on election interference. That requires more than the two parties taking actions that were informed by or responsive to the other's actions or interests. We applied the term coordination in that sense when stating in the report that the investigation did not establish that the Trump Campaign coordinated with the Russian government in its election interference activities.

The report on our investigation consists of two volumes:

Volume I describes the factual results of the Special Counsel's investigation of Russia's interference in the 2016 presidential election and its interactions with the Trump Campaign. Section I describes the scope of the investigation. Sections II and III describe the principal ways Russia interfered in the 2016 presidential election. Section IV describes links between the Russian government and individuals associated with the Trump Campaign. Section V sets forth the Special Counsel's charging decisions.

Volume II addresses the President's actions towards the FBI's investigation into Russia's interference in the 2016 presidential election and related matters, and his actions towards the Special Counsel's investigation. Volume II separately states its framework and the considerations that guided that investigation.

Executive Summary to Volume I

Russian Social Media Campaign

The Internet Research Agency (IRA) carried out the earliest Russian interference operations identified by the investigation - a social media campaign designed to provoke and amplify political and social discord in the United States. The IRA was based in St. Petersburg, Russia, and received funding from Russian oligarch Yevgeniy Prigozhin and companies he controlled. Prigozhin is widely reported to have ties to Russian President Vladimir Putin, [redacted]

In mid-2014, the IRA sent employees to the United States on an intelligence-gathering mission with instructions [redacted].

The IRA later used social media accounts and interest groups to sow discord in the U.S. political system through what it termed "information warfare." The campaign evolved from a generalized program designed in 2014 and 2015 to undermine the U.S. electoral system, to a targeted operation that by early 2016 favored candidate Trump and disparaged candidate Clinton. The IRA's operation also included the purchase of political advertisements on social media in the names of U.S. persons and entities, as well as the staging of political rallies inside the United States. To organize those rallies, IRA employees posed as U.S. grassroots entities and persons and made contact with Trump supporters and Trump Campaign officials in the United States. The investigation did not identify evidence that any U.S. persons conspired or coordinated with the IRA. Section II of this report details the Office's investigation of the Russian social media campaign.

Russian Hacking Operations

At the same time that the IRA operation began to focus on supporting candidate Trump in early 2016, the Russian government employed a second form of interference: cyber intrusions (hacking) and releases of hacked materials damaging to the Clinton Campaign. The Russian intelligence service known as the Main Intelligence Directorate of the General Staff of the Russian Army (GRU) carried out these operations.

In March 2016, the GRU began hacking the email accounts of Clinton Campaign volunteers and employees, including campaign chairman John Podesta.

In April 2016, the GRU hacked into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). The GRU stole hundreds of thousands of documents from the compromised email accounts and networks. Around the time that the DNC announced in mid-June 2016 the Russian government's role in hacking its network, the GRU began disseminating stolen materials through the fictitious online personas "DCLeaks" and "Guccifer 2.0." The GRU later released additional materials through the organization WikiLeaks.

The presidential campaign of Donald J. Trump ("Trump Campaign" or "Campaign") showed interest in WikiLeaks's releases of documents and welcomed their potential to damage candidate Clinton. Beginning in June 2016, [redacted] forecast to senior Campaign officials that WikiLeaks would release information damaging to candidate Clinton. WikiLeaks's first release came in July 2016. Around the same time, candidate Trump announced that he hoped Russia would recover emails described as missing from a private server used by Clinton when she was Secretary of State (he later said that he was speaking sarcastically). [redacted] WikiLeaks began releasing Podesta's stolen emails on October 7, 2016, less than one hour after a U.S. media outlet released video considered damaging to candidate Trump. Section III of this Report details the Office's investigation into the Russian hacking operations, as well as other efforts by Trump Campaign supporters to obtain Clinton-related emails.

Russian Contacts with the Campaign

The social media campaign and the GRU hacking operations coincided with a series of contacts between Trump Campaign officials and individuals with ties to the Russian government. The Office investigated whether those contacts reflected or resulted in the Campaign conspiring or coordinating with Russia in its election-interference activities. Although the investigation established that the Russian government perceived it would benefit from a Trump presidency and worked to secure that outcome, and that the Campaign expected it would benefit electorally from information stolen and released through Russian efforts, the investigation did not establish that members of the Trump Campaign conspired or coordinated with the Russian government in its election interference activities.

The Russian contacts consisted of business connections, offers of assistance to the Campaign, invitations for candidate Trump and Putin to meet in person,

invitations for Campaign officials and representatives of the Russian government to meet, and policy positions seeking improved U.S.-Russian relations. Section IV of this Report details the contacts between Russia and the Trump Campaign during the campaign and transition periods, the most salient of which are summarized below in chronological order.

2015. Some of the earliest contacts were made in connection with a Trump Organization real-estate project in Russia known as Trump Tower Moscow. Candidate Trump signed a Letter of Intent for Trump Tower Moscow by November 2015, and in January 2016 Trump Organization executive Michael Cohen emailed and spoke about the project with the office of Russian government press secretary Dmitry Peskov. The Trump Organization pursued the project through at least June 2016, including by considering travel to Russia by Cohen and candidate Trump.

Spring 2016. Campaign foreign policy advisor George Papadopoulos made early contact with Joseph Mifsud, a London-based professor who had connections to Russia and traveled to Moscow in April 2016. Immediately upon his return to London from that trip, Mifsud told Papadopoulos that the Russian government had "dirt" on Hillary Clinton in the form of thousands of emails. One week later, in the first week of May 2016, Papadopoulos suggested to a representative of a foreign government that the Trump Campaign had received indications from the Russian government that it could assist the Campaign through the anonymous release of information damaging to candidate Clinton. Throughout that period of time and for several months thereafter, Papadopoulos worked with Mifsud and two Russian nationals to arrange a meeting between the Campaign and the Russian government. No meeting took place.

Summer 2016. Russian outreach to the Trump Campaign continued into the summer of 2016, as candidate Trump was becoming the presumptive Republican nominee for President. On June 9, 2016, for example, a Russian lawyer met with senior Trump Campaign officials Donald Trump Jr., Jared Kushner, and campaign chairman Paul Manafort to deliver what the email proposing the meeting had described as "official documents and information that would incriminate Hillary." The materials were offered to Trump Jr. as "part of Russia and its government's support for Mr. Trump." The written communications setting up the meeting showed that the Campaign anticipated receiving information from Russia that could assist candidate Trump's electoral prospects, but the Russian lawyer's presentation did not provide such information.

Days after the June 9 meeting, on June 14, 2016, a cybersecurity firm and the DNC announced that Russian government hackers had infiltrated the DNC and obtained access to opposition research on candidate Trump, among other

documents.

In July 2016, Campaign foreign policy advisor Carter Page traveled in his personal capacity to Moscow and gave the keynote address at the New Economic School. Page had lived and worked in Russia between 2003 and 2007. After returning to the United States, Page became acquainted with at least two Russian intelligence officers, one of whom was later charged in 2015 with conspiracy to act as an unregistered agent of Russia. Page's July 2016 trip to Moscow and his advocacy for pro-Russian foreign policy drew media attention. The Campaign then distanced itself from Page and, by late September 2016, removed him from the Campaign.

July 2016 was also the month WikiLeaks first released emails stolen by the GRU from the DNC. On July 22, 2016, WikiLeaks posted thousands of internal DNC documents revealing information about the Clinton Campaign. Within days, there was public reporting that U.S. intelligence agencies had "high confidence" that the Russian government was.behind the theft of emails and documents from the DNC. And within a week of the release, a foreign government informed the FBI about its May 2016 interaction with Papadopoulos and his statement that the Russian government could assist the Trump Campaign. On July 31, 2016, based on the foreign government reporting, the FBI opened an investigation into potential coordination between the Russian government and individuals associated with the Trump Campaign.

Separately, on August 2, 2016, Trump campaign chairman Paul Manafort met in New York City with his long-time business associate Konstantin Kilimnik, who the FBI assesses to have ties to Russian intelligence. Kilimnik requested the meeting to deliver in person a peace plan for Ukraine that Manafort acknowledged to the Special Counsel's Office was a "backdoor" way for Russia to control part of eastern Ukraine; both men believed the plan would require candidate Trump's assent to succeed (were he to be elected President). They also discussed the status of the Trump Campaign and Manafort's strategy for winning Democratic votes in Midwestern states. Months before that meeting, Manafort had caused internal polling data to be shared with Kilimnik, and the sharing continued for some period of time after their August meeting.

Fall 2016. On October 7, 2016, the media released video of candidate Trump speaking in graphic terms about women years earlier, which was considered damaging to his candidacy. Less than an hour later, WikiLeaks made its second release: thousands of John Podesta' s emails that had been stolen by the GRU in late March 2016. The FBI and other U.S. government institutions were at the time continuing their investigation of suspected Russian government efforts to

interfere in the presidential election. That same day, October 7, the Department of Homeland Security and the Office of the Director of National Intelligence issued a joint public statement "that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations." Those "thefts" and the "disclosures" of the hacked materials through online platforms such as WikiLeaks, the statement continued, "are intended to interfere with the US election process."

Post-2016 Election. Immediately after the November 8 election, Russian government officials and prominent Russian businessmen began trying to make inroads into the new administration. The most senior levels of the Russian government encouraged these efforts. The Russian Embassy made contact hours after the election to congratulate the President-Elect and to arrange a call with President Putin. Several Russian businessmen picked up the effort from there.

Kirill Dmitriev, the chief executive officer of Russia's sovereign wealth fund, was among the Russians who tried to make contact with the incoming administration. In early December, a business associate steered Dmitriev to Erik Prince, a supporter of the Trump Campaign and an associate of senior Trump advisor Steve Bannon. Dmitriev and Prince later met face-to-face in January 2017 in the Seychelles and discussed U.S.-Russia relations. During the same period, another business associate introduced Dmitriev to a friend of Jared Kushner who had not served on the Campaign or the Transition Team. Dmitriev and Kushner's friend collaborated on a short written reconciliation plan for the United States and Russia, which Dmitriev implied had been cleared through Putin. The friend gave that proposal to Kushner before the inauguration, and Kushner later gave copies to Bannon and incoming Secretary of State Rex Tillerson.

On December 29, 2016, then-President Obama imposed sanctions on Russia for having interfered in the election. Incoming National Security Advisor Michael Flynn called Russian Ambassador Sergey Kislyak and asked Russia not to escalate the situation in response to the sanctions. The following day, Putin announced that Russia would not take retaliatory measures in response to the sanctions at that time. Hours later, President-Elect Trump tweeted, "Great move on delay (by V. Putin)." The next day, on December 31, 2016, Kislyak called Flynn and told him the request had been received at the highest levels and Russia had chosen not to retaliate as a result of Flynn's request.

On January 6, 2017, members of the intelligence community briefed President-Elect Trump on a joint assessment-drafted and coordinated among the

Central Intelligence Agency, FBI, and National Security Agency-that concluded with high confidence that Russia had intervened in the election through a variety of means to assist Trump's candidacy and harm Clinton's. A declassified version of the assessment was publicly released that same day.

Between mid-January 2017 and early February 2017, three congressional committees-the House Permanent Select Committee on Intelligence (HPSCI), the Senate Select Committee on Intelligence (SSCI), and the Senate Judiciary Committee (SJC)-announced that they would conduct inquiries, or had already been conducting inquiries, into Russian interference in the election. Then-FBI Director James Corney later confirmed to Congress the existence of the FBI's investigation into Russian interference that had begun before the election. On March 20, 2017, in open-session testimony before HPSCI, Corney stated:

> I have been authorized by the Department of Justice to confirm that the FBI, as part of our counterintelligence mission, is investigating the Russian government's efforts to interfere in the 2016 presidential election, and that includes investigating the nature of any links between individuals associated with the Trump campaign and the Russian government and whether there was any coordination between the campaign and Russia's efforts. ... As with any counterintelligence investigation, this will also include an assessment of whether any crimes were committed.

The investigation continued under then-Director Corney for the next seven weeks until May 9, 2017, when President Trump fired Corney as FBI Director-an action which is analyzed in Volume II of the report.

On May 17, 2017, Acting Attorney General Rod Rosenstein appointed the Special Counsel and authorized him to conduct the investigation that Corney had confirmed in his congressional testimony, as well as matters arising directly from the investigation, and any other matters within the scope of 28 C.F.R. §600.4(a), which generally covers efforts to interfere with or obstruct the investigation.

President Trump reacted negatively to the Special Counsel's appointment. He told advisors that it was the end of his presidency, sought to have Attorney General Jefferson (Jeff) Sessions unrecuse from the Russia investigation and to have the Special Counsel removed, and engaged in efforts to curtail the Special Counsel's investigation and prevent the disclosure of evidence to it, including through public and private contacts with potential witnesses. Those and related actions are described and analyzed in Volume II of the report.

The Special Counsel's Charging Decisions

In reaching the charging decisions described in Volume 1 of the report, the Office determined whether the conduct it found amounted to a violation of federal criminal law chargeable under the Principles of Federal Prosecution. See Justice Manual §9-27.000 et seq. (2018). The standard set forth in the Justice Manual is whether the conduct constitutes a crime; if so, whether admissible evidence would probably be sufficient to obtain and sustain a conviction; and whether prosecution would serve a substantial federal interest that could not be adequately served by prosecution elsewhere or through non-criminal alternatives. See Justice Manual §9-27 .220.

Section V of the report provides detailed explanations of the Office's charging decisions, which contain three main components.

First, the Office determined that Russia's two principal interference operations in the 2016 U.S. presidential election-the social media campaign and the hacking-and-dumping operations-violated U.S. criminal law. Many of the individuals and entities involved in the social media campaign have been charged with participating in a conspiracy to defraud the United States by undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections, as well as related counts of identity theft. See ***United States v. Internet Research Agency, et al.***, No. 18-cr-32 (D.D.C.). Separately, Russian intelligence officers who carried out the hacking into Democratic Party computers and the personal email accounts of individuals affiliated with the Clinton Campaign conspired to violate, among other federal laws, the federal computer-intrusion statute, and they have been so charged. ***See United States v. Netyksho, et al.***, No. 18-cr-215 (D.D.C.).

[redacted].

Second, while the investigation identified numerous links between individuals with ties to the Russian government and individuals associated with the Trump Campaign, the evidence was not sufficient to support criminal charges. Among other things, the evidence was not sufficient to charge any Campaign official as an unregistered agent of the Russian government or other Russian principal. And our evidence about the June 9, 2016 meeting and WikiLeaks' s releases

of hacked materials was not sufficient to charge a criminal campaign-finance violation. Further, the evidence was not sufficient to charge that any member of the Trump Campaign conspired with representatives of the Russian government to interfere in the 2016 election.

Third, the investigation established that several individuals affiliated with the Trump Campaign lied to the Office, and to Congress, about their interactions with Russian-affiliated individuals and related matters. Those lies materially impaired the investigation of Russian election interference. The Office charged some of those lies as violations of the federal false-statements statute. Former National Security Advisor Michael Flynn pleaded guilty to lying about his interactions with Russian Ambassador Kislyak during the transition period. George Papadopoulos, a foreign policy advisor during the campaign period, pleaded guilty to lying to investigators about, inter alia, the nature and timing of his interactions with Joseph Mifsud, the professor who told Papadopoulos that the Russians had dirt on candidate Clinton .in the form of thousands of emails. Former Trump Organization attorney Michael Cohen pleaded guilt to making false statements to Congress about the Trump Moscow project. [redacted]. And in February 2019, the U.S. District Court for the District of Columbia found that Manafort lied to the Office and the grand jury concerning his interactions and communications with Konstantin Kilimnik about Trump Campaign polling data and a peace plan for Ukraine.

The Office investigated several other events that have been publicly repot1ed to involve potential Russia-related contacts. For example, the investigation established that interactions between Russian Ambassador Kislyak and Trump Campaign officials both at the candidate's April 2016 foreign policy speech in Washington, D.C., and during the week of the Republican National Convention were brief, public, and non-substantive. And the investigation did not establish that one Campaign official's efforts to dilute a portion of the Republican Party platform on providing assistance to Ukraine were undertaken at the behest of candidate Trump or Russia. The investigation also did not establish that a meeting between Kislyak and Sessions in September 2016 at Sessions's Senate office included any more than a passing mention of the presidential campaign.

The investigation did not always yield admissible information or testimony, or a complete picture of the activities undertaken by subjects of the investigation.

Some individuals invoked their Fifth Amendment right against compelled self-incrimination and were not, in the Office' s judgment, appropriate candidates for grants of immunity. The Office limited its pursuit of other witnesses and information-such as information known to attorneys or individuals claiming to be members of the media-in light of internal Depa11ment of Justice policies. See, e.g., Justice Manual§§9-13.400, 13.410. Some of the information obtained via court process, moreover, was presumptively covered by legal privilege and was screened from investigators by a filter (or "taint") team. Even when individuals testified or agreed to be interviewed, they sometimes provided information that was false or incomplete, leading to some of the false-statements charges described above. And the Office faced practical limits on its ability to access relevant evidence as well-numerous witnesses and subjects lived abroad, and documents were held outside the United States.

Further, the Office learned that some of the individuals we interviewed or whose conduct we investigated - including some associated with the Trump Campaign - deleted relevant communications or communicated during the relevant period using applications that feature encryption or that do not provide for long-term retention of data or communications records. In such cases, the Office was not able to corroborate witness statements through comparison to contemporaneous communications or fully question witnesses about statements that appeared inconsistent with other known facts.

Accordingly, while this report embodies factual and legal determinations that the Office believes to be accurate and complete to the greatest extent possible, given these identified gaps, the Office cannot rule out the possibility that the unavailable information would shed additional light on (or cast in a new light) the events described in the report.

I. The Special Counsel's Investigation

On May 17, 2017, Deputy Attorney General Rod J. Rosenstein-then serving as Acting Attorney General for the Russia investigation following the recusal of former Attorney General Jeff Sessions on March 2, 2016-appointed the Special Counsel "to investigate Russian interference with the 2016 presidential election and related matters." Office of the Deputy Att'y Gen., Order No. 3915-2017, Appointment of Special Counsel to Investigate Russian Interference with the 2016 Presidential Election and Related Matters, May 17, 2017) ("Appointment Order"). Relying on "the authority vested" in the Acting Attorney General," including 28 U.S.C. §§509, 510, and 515," the Acting Attorney General ordered the appointment of a Special Counsel " in order to discharge [the Acting Attorney General' s] responsibility to provide supervision and management of the Department of Justice, and to ensure a full and thorough investigation of the Russian government's efforts to interfere in the 2016 presidential election." Appointment Order (introduction). "The Special Counsel," the Order stated, "is authorized to conduct the investigation confirmed by then-FBI Director James B. Corney in testimony before the House Permanent Select Committee on Intelligence on March 20, 2017," including:

i any links and/or coordination between the Russian government and individuals associated with the campaign of President Donald Trump; and

ii any matters that arose or may arise directly from the investigation; and

iii any other matters within the scope of 28 C.F.R. §600.4(a).

Appointment Order ¶(b). Section 600.4 affords the Special Counsel "the authority to investigate and prosecute federal crimes committed in the course of, and with intent to interfere with, the Special Counsel's investigation, such as perjury, obstruction of justice, destruction of evidence, and intimidation of witnesses." 28 C.F.R. §600.4(a). The authority to investigate "any matters that arose ... directly from the investigation," Appointment Order ¶(b)(ii), covers similar crimes that may have occurred during the course of the FBI's confirmed investigation before the Special Counsel's appointment. "If the Special Counsel believes it is necessary and appropriate," the Order further provided, "the Special Counsel is authorized to prosecute federal crimes arising from the investigation of these matters." Id. ¶(c). Finally, the Acting Attorney General made applicable

" Sections 600.4 through 600.10 of Title 28 of the Code of Federal Regulations." Id. ¶(d).

The Acting Attorney General further clarified the scope of the Special Counsel's investigatory authority in two subsequent memoranda. A memorandum dated August 2, 2017, explained that the Appointment Order had been "worded categorically in order to permit its public release without confirming specific investigations involving specific individuals." It then confirmed that the Special Counsel had been authorized since his appointment to investigate allegations that three Trump campaign officials-Carter Page, Paul Manafort, and George Papadopoulos-"committed a crime or crimes by colluding with Russian government officials with respect to the Russian government's efforts to interfere with the 2016 presidential election." The memorandum also confirmed the Special Counsel's authority to investigate certain other matters, including two additional sets of allegations involving Manafort (crimes arising from payments he received from the Ukrainian government and crimes arising from his receipt of loans from a bank whose CEO was then seeking a position in the Trump Administration); allegations that Papadopoulos committed a crime or crimes by acting as an unregistered agent of the Israeli government; and four sets of allegations involving Michael Flynn, the former National Security Advisor to President Trump.

On October 20, 2017, the Acting Attorney General confirmed in a memorandum the Special Counsel's investigative authority as to several individuals and entities. First," as part of a full and thorough investigation of the Russian government's efforts to interfere in the 2016 presidential election," the Special Counsel was authorized to investigate "the pertinent activities of Michael Cohen, Richard Gates, [redacted] Roger Stone, and [redacted]" "Confirmation of the authorization to investigate such individuals," the memorandum stressed, "does not suggest that the Special Counsel has made a determination that any of them has committed a crime." Second, with respect to Michael Cohen, the memorandum recognized the Special Counsel's authority to investigate "leads relate[d] to Cohen's establishment and use of Essential Consultants LLC to, inter alia, receive funds from Russian-backed entities." Third, the memorandum memorialized the Special Counsel's authority to investigate individuals and entities who were possibly engaged in "jointly undertaken activity" with existing subjects of the investigation, including Paul Manafort. Finally, the memorandum described an FBI investigation opened before the Special Counsel's appointment into "allegations that [then-Attorney General Jeff Sessions] made false statements to the United States Senate[,]" and confirmed the Special Counsel's authority to investigate that matter.

I. THE SPECIAL COUNSEL'S INVESTIGATION

The Special Counsel structured the investigation in view of his power and authority "to exercise all investigative and prosecutorial functions of any United States Attorney." 28 C.F.R: § 600.6. Like a U.S. Attorney's Office, the Special Counsel's Office considered a range of classified and unclassified information available to the FBI in the course of the Office's Russia investigation, and the Office structured that work around evidence for possible use in prosecutions of federal crimes (assuming that one or more crimes were identified that warranted prosecution). There was substantial evidence immediately available to the Special Counsel at the inception of the investigation in May 2017 because the FBI had, by that time, already investigated Russian election interference for nearly 10 months. The Special Counsel's Office exercised its judgment regarding what to investigate and did not, for instance, investigate every public report of a contact between the Trump Campaign and Russian-affiliated individuals and entities.

The Office has concluded its investigation into links and coordination between the Russian government and individuals associated with the Trump Campaign. Certain proceedings associated with the Office's work remain ongoing. After consultation with the Office of the Deputy Attorney General, the Office has transferred responsibility for those remaining issues to other components of the Department of Justice and FBI. Appendix D lists those transfers.

Two district courts confirmed the breadth of the Special Counsel's authority to investigate Russia election interference and links and/or coordination with the Trump Campaign. See United States v. Manafort, 312 F. Supp. 3d 60, 79-83 (D.D.C. 2018); United States v. Manafort, 321 F. Supp. 3d 640, 650-655 (E.D. Va. 2018). In the course of conducting that investigation, the Office periodically identified evidence of potential criminal activity that was outside the scope of the Special Counsel's authority established by the Acting Attorney General. After consultation with the Office of the Deputy Attorney General, the Office referred that evidence to appropriate law enforcement authorities, principally other components of the Department of Justice and to the FBI. Appendix D summarizes those referrals.

To carry out the investigation and prosecution of the matters assigned to him, the Special Counsel assembled a team that at its high point included 19 attorneys-five of whom joined the Office from private practice and 14 on detail or assigned from other Department of Justice components. These attorneys were assisted by a filter team of Department lawyers and FBI personnel who screened

materials obtained via court process for privileged information before turning those materials over to investigators; a support staff of three paralegals on detail from the Department's Antitrust Division; and an administrative staff of nine responsible for budget, finance, purchasing, human resources, records, facilities, security, information technology, and administrative support. The Special Counsel attorneys and support staff were co-located with and worked alongside approximately 40 FBI agents, intelligence analysts, forensic accountants, a paralegal, and professional staff assigned by the FBI to assist the Special Counsel's investigation. Those "assigned" FBI employees remained under FBI supervision at all times; the matters on which they assisted were supervised by the Special Counsel.[1]

During its investigation the Office issued more than 2,800 subpoenas under the auspices of a grand jury sitting in the District of Columbia; executed nearly 500 search-and-seizure warrants; obtained more than 230 orders for communications records under 18 U.S.C. § 2703(d); obtained almost 50 orders authorizing use of pen registers; made 13 requests to foreign governments pursuant to Mutual Legal Assistance Treaties; and interviewed approximately 500 witnesses, including almost 80 before a grand jury.

From its inception, the Office recognized that its investigation could identify foreign intelligence and counterintelligence information relevant to the FBI's broader national security mission. FBI personnel who assisted the Office established procedures to identify and convey such information to the FBI. The FBI's Counterintelligence Division met with the Office regularly for that purpose for most of the Office's tenure. For more than the past year, the FBI also embedded personnel at the Office who did not work on the Special Counsel's investigation, but whose purpose was to review the results of the investigation and to send-in writing-summaries of foreign intelligence and counterintelligence information to FBIHQ and FBI Field Offices. Those communications and other correspondence between the Office and the FBI contain information derived from the investigation, not all of which is contained in this Volume. This Volume is a summary. It

[1] FBI personnel assigned to the Special Counsel's Office were required to adhere to all applicable federal law and all Department and FBI regulations, guidelines, and policies. An FBI attorney worked on FBI-related matters for the Office, such as FBI compliance with all FBI policies and procedures, including the FBI's Domestic Investigations and Operations Guide (DIOG). That FBI attorney worked under FBI legal supervision, not the Special Counsel's supervision.

contains, in the Office's judgment, that information necessary to account for the Special Counsel's prosecution and declination decisions and to describe the investigation's main factual results.

II. Russian "Active Measures" Social Media Campaign

The first form of Russian election influence came principally from the Internet Research Agency, LLC (IRA), a Russian organization funded by Yevgeniy Viktorovich Prigozhin and companies he controlled, including Concord Management and Consulting LLC and Concord Catering (collectively "Concord").[2] The IRA conducted social media operations targeted at large U.S. audiences with the goal of sowing discord in the U.S. political system.[3] These operations constituted "active measures" (активные мероприятия), a term that typically refers to operations conducted by Russian security services aimed at influencing the course of international affairs.[4]

The IRA and its employees began operations targeting the United States as early as 2014. Using fictitious U.S. personas, IRA employees operated social media accounts and group pages designed to attract U.S. audiences. These groups and accounts, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists. Over time, these social media accounts became a means to reach large U.S. audiences. IRA employees travelled to the United States in mid-2014 on an intelligence-gathering mission to obtain information and photographs for use in their social media posts.

IRA employees posted derogatory information about a number of candidates in the 2016 U.S. presidential election. By early to mid-2016, IRA operations included supporting the Trump Campaign and disparaging candidate Hillary Clinton. The IRA made various expenditures to carry out those activities, including buying political advertisements on social media in the names of U.S. persons and entities. Some IRA employees, posing as U.S. persons and without revealing their Russian

[2]The Office is aware of reports that other Russian entities engaged in similar active measures operations targeting the United States. Some evidence collected by the Office corroborates those reports, and the Office has shared that evidence with other offices in the Department of Justice and FBI.

[3] [redacted] see also SM-2230634, serial 44 (analysis). The FBI case number cited here, and other FBI case numbers identified in the report, should be treated as law enforcement sensitive given the context. The report contains additional law enforcement sensitive information.

[4]As discussed in Part V below, the active measures investigation has resulted in criminal charges against 13 individual Russian nationals and three Russian entities, principally for conspiracy to defraud the United States, in violation of 18 U.S.C. § 371. See Volume I, Section V.A, infra; Indictment, United States v. Internet Research Agency, et al., 1 :18-cr-32 (D.D.C. Feb. 16, 2018), Doc. 1 ("Internet Research Agency Indictment").

association, communicated electronically with individuals associated with the Trump Campaign and with other political activists to seek to coordinate political activities, including the staging of political rallies.[5] The investigation did not identify evidence that any U.S. persons knowingly or intentionally coordinated with the IRA's interference operation.

By the end of the 2016 U.S. election, the IRA had the ability to reach millions of U.S. persons through their social media accounts. Multiple IRA-controlled Facebook groups and Instagram accounts had hundreds of thousands of U.S. participants. IRA-controlled Twitter accounts separately had tens of thousands of followers, including multiple U.S. political figures who retweeted IRA-created content. In November 2017, a Facebook representative testified that Facebook had identified 470 IRA-controlled Facebook accounts that collectively made 80,000 posts between January 2015 and August 2017. Facebook estimated the IRA reached as many as 126 million persons through its Face book accounts.[6] In January 2018, Twitter announced that it had identified 3,814 IRA-controlled Twitter accounts and notified approximately 1 .4 million people Twitter believed may have been in contact with an iRA-controlled account.[7]

A. Structure of the Internet Research Agency

[redacted][8] [redacted][9]

[5]Internet Research Agency Indictment §§52, 54, 55(a), 56, 74; [redacted]

[6]Social Media Influence in the 2016 US. Election, Hearing Before the Senate Select Committee on Intelligence, 115th Cong. 13 (11/1/17) (testimony of Colin Stretch, General Counsel of Facebook) ("We estimate that roughly 29 million people were served content in their News Feeds directly from the IRA's 80,000 posts over the two years. Posts from these Pages were also shared, liked, and followed by people on Facebook, and, as a result, three times more people may have been exposed to a story that originated from the Russian operation. Our best estimate is that approximately 126 million people may have been served content from a Page associated with the IRA at some point during the two-year period."). The Facebook representative also testified that Facebook had identified 170 Instagram accounts that posted approximately 120,000 pieces of content during that time. Facebook did not offer an estimate of the audience reached via Instagram.

[7]Twitter, Update on Twitter's Review of the 2016 US Election (Jan. 31, 2018).

[8]See SM-2230634, serial 92.

[9][redacted]

II. RUSSIAN "ACTIVE MEASURES" SOCIAL MEDIA CAMPAIGN

[redacted][10]

The organization quickly grew. [redacted][11] [redacted][12]

The growth of the organization also led to a more detailed organizational structure. [redacted].[13]

Two individuals headed the IRA's management: its general director, Mikhail Bystrov, and its executive director, Mikhail Burchik. [redacted][14] [redacted][15]

As early as spring of 2014, the IRA began to hids its funding and activities. [redacted].[16]

The IRA's U.S. operations are part of a larger set of interlocking operations

[10] [redacted]

[11] See SM-2230634, serial 86 [redacted]

[12] [redacted]

[13] [redacted]

[14] See, e.g., SM-2230634, serials 9, 113 & 180 [redacted]

[15] [redacted]

[16] [redacted]. See SM-2230634, serials 131 & 204.

known as "Project Lakhta," [redacted][17] [redacted][18]

B. Funding and Oversight from Concord and Prigozhin

Until at least February 2018, Yevgeniy Viktorovich Prigozhin and two Concord companies funded the IRA. Prigozhin is a wealthy Russian businessman who served as the head of Concord. [redacted] Prigozhin was sanctioned by the U.S. Treasury Deparment in December 2016,[19] [redacted][20] [redacted][21] Numerous media sources have reported on Prigozhin's ties to Putin, and the two have appeared together in public photographs.[22]

[redacted][23]

[redacted][24]

[redacted][25]

[17] [redacted]

[18] [redacted]

[19] U.S. Treasury Deprutment, "Treasury Sanctions Individuals and Entities in Connection with Russia's Occupation of Crimea and the Conflict in Ukraine" (Dec. 20, 2016).

[20] [redacted]

[21] [redacted]

[22] See, e.g., Neil MacFarquhar, Yevgeny Prigozhin, Russian Oligarch Indicted by US., Is Known as "Putin's Cook", New York Times (Feb. 16, 2018).

[23] [redacted]

[24] [redacted]

[25] [redacted] see also SM-2230634, serial 113 [redacted]

II. RUSSIAN "ACTIVE MEASURES" SOCIAL MEDIA CAMPAIGN

[redacted]

[redacted][26] [redacted][27]

[redacted]

[redacted][28] [redacted]

IRA employees were aware that Prigozhin was involved in the IRA's U.S. operations, [redacted][29] [redacted][30] In May 2016, IRA employees, claiming to be U.S. social activists and administrators of Facebook groups, recruited U.S. persons to hold signs (including one in front of the White House) that read "Happy 55th Birthday Dear Boss," as an homage to Prigozhin (whose 55th birthday was on June 1, 2016).[31] [redacted][32]

[26] [redacted]

[27] [redacted]

[28] The term "troll" refers to internet users - in this context, paid operatives - who post inflammatory or otherwise disruptive content on social media or other websites.

[29] [redacted]. See SM-2230634, serials 131 & 204.

[30] See SM-2230634, serial 156.

[31] Internet Research Agency Indictment ¶12(b); ***see also*** 5/26/16 Facebook Messages, ID 1479936895656747 (United Muslims of America) & [redacted]

[32] [redacted] see also SM-2230634, serial 189. [redacted].

[redacted]

C. The IRA Targets U.S. Elections

1. The IRA Ramps Up U.S. Operations as Early as 2014

The IRA's U.S. operatiosn sought to influence public opinion through online media and forums. By the spring of 2014, the IRA began to consolidate U.S. operations within a single general department, known internally as the "Translator" (переводчик) department. [redacted] IRA subdivided the Translator Department into different responsibilities, ranging from operations on different social media platforms to analytics to graphics and IT.

[redacted][33] [redacted][34]

[redacted]

[redacted][35] [redacted][36]

[redacted]

[redacted]

[33] 33
[34] 34
[35] 35
[36] 36

II. RUSSIAN "ACTIVE MEASURES" SOCIAL MEDIA CAMPAIGN

[redacted][37]

IRA employees also traveled to the United States on intelligence-gathering missions. In June 2014, four IRA employees applied to the U.S. Department of State to enter the United States, while lying about the purpose of their trip and claiming to be four friends who had met at a party.[38] Ultimately, two IRA employees-Anna Bogacheva and Aleksandra Krylova-received visas and entered the United States on June 4, 2014.

Prior to traveling, Krylova and Bogacheva compiled itineraries and instructions for the trip. [redacted][39] [redacted][40] [redacted][41]

2. U.S. Operations Through IRA-Controlled Social Media Accounts

Dozens of IRA employees were responsible for operating accounts and personas on different U.S. social media platforms. The IRA referred to employees assigned to operate the social media accounts as "specialists."[42] Starting as early as 2014, the IRA's U.S. operations included social media specialists focusing on Facebook, YouTube, and Twitter.[43] The IRA later added specialists who operated on Tumblr and Instagram accounts.[44]

[37] 37
[38] 38
[39] 39
[40] 40
[41] 41
[42] 42
[43] 43
[44] 44

II. RUSSIAN "ACTIVE MEASURES" SOCIAL MEDIA CAMPAIGN

Initially, the IRA created social media accounts that pretended to be the personal accounts of U.S. persons.[45] By early 2015, the IRA began to create larger social media groups or public social media pages that claimed (falsely) to be affiliated with U.S. political and grassroots organizations. In certain cases, the IRA created accounts that mimicked real U.S. organizations. For example, one IRA-controlled Twitter account, @TEN_GOP, purported to be connected to the Tennessee Republican Party.[46] More commonly, the IRA created accounts in the names of fictitious U.S. organizations and grassroots groups and used these accounts to pose as anti-immigration groups, Tea Party activists, Black Lives Matter protestors, and other U.S. social and political activists.

The IRA closely monitored the activity of its social media accounts. [redacted].[47] [redacted][48]

[redacted]

By February 2016, internal IRA documents referred to support for the Trump Campaign and opposition to candidate Clinton.[49] For example, [redacted] directions to IRA operators [redacted]. "Main idea: Use any opportunity to criticize Hillary [Clinton] and the rest (except Sanders and Trump - we support them)."[50] [redacted]

[45] 45
[46] 46
[47] 47
[48] 48
[49] 49
[50] 50

II. RUSSIAN "ACTIVE MEASURES" SOCIAL MEDIA CAMPAIGN

The focus on the U.S. presidential campaign continued through 2016. In [redacted] 2016 internal [redacted] reviewing the IRA-controlled Facebook group "Secured Borders," the author criticized the "lower number of posts dedicated to criticizing Hillary Clinton" and reminded the Facebook specialist "it is imperative to intensify criticizing Hillary Clinton."[51]

IRA employees also acknowledged that their work focused on influencing the U.S. presidential election. [redacted][52]

3. U.S. Operations Through Facebook

Many IRA operations used Facebook accounts created and operated by its specialists. [redacted]

i [redacted]

ii [redacted]

iii [redacted]

[redacted][53]

[redacted]

[51] 51
[52] 52
[53] 53

II. RUSSIAN "ACTIVE MEASURES" SOCIAL MEDIA CAMPAIGN

[redacted].[54] The IRA Facebook groups active during the 2016 campaign covered a range of political issues and included purported conservative groups (with names such as "Being Patriotic," "Stop All Immigrants," "Secured Borders," and "Tea Party News"), purported Black social justice groups ("Black Matters," "Blacktivist," and "Don't Shoot Us"), LGBTQ groups ("LGBT United"), and religious groups ("United Muslims of America").

Throughout 2016, IRA accounts published an increasing number of materials supporting the Trump Campaign and opposing the Clinton Campaign. For example, on May 31, 2016, the operational account "Matt Skiber" began to privately message dozens of pro-Trump Facebook groups asking them to help plan a "pro-Trump rally near Trump Tower."[55]

To reach larger U.S. audiences, the IRA purchased advertisements from Facebook that promoted the IRA groups on the newsfeeds of U.S. audience members. According to Facebook, the IRA purchased over 3,500 advertisements, and the expenditures totaled approximately $100,000.[56]

During the U.S. presidential campaign, many IRA-purchased advertisements explicitly supported or opposed a presidential candidate or promoted U.S. rallies organized by the IRA (discussed below). As early as March 2016, the IRA purchased advertisements that overtly opposed the Clinton Campaign. For example, on March 18, 2016, the IRA purchased an advertisement depicting candidate Clinton and a caption that read in part, "If one day God lets this liar enter the White House as a president - that day would be a real national tragedy."[57] Similarly, on April 6, 2016, the IRA purchased advertisements for its account "Black Matters" calling for a "flashmob" of U.S. persons to "take a photo with #HillaryClintonForPrison2016 or #nohillary2016."[58] IRA-purchased advertisements featuring Clinton were, with very few exceptions, negative.[59]

IRA-purchased advertisements referencing candidate Trump largely supported his campaign. The first known IRA advertisement explicitly endorsing the Trump Campaign was purchased on April 19, 2016. The IRA bought an advertisement for its Instagram account "Tea Party News" asking U.S. persons to help them "make a patriotic team of young Trump supporters" by uploading photos with the

[54] 54
[55] 55
[56] 56
[57] 57
[58] 58
[59] 59

hashtag "#KIDS4TRUMP."[60] In subsequent months, the IRA purchased dozens of advertisements supporting the Trump Campaign, predominantly through the Facebook groups "Being Patriotic," "Stop All Invaders," and "Secured Borders."

Collectively, the IRA's social media accounts reached tens of millions of U.S. persons. Individual IRA social media accounts attracted hundreds of thousands of followers. For example, at the time they were deactivated by Facebook in mid-2017, the IRA's "United Muslims of America" Facebook group had over 300,000 followers, the "Don't Shoot Us" Facebook group had over 250,000 followers, the "Being Patriotic" Facebook group had over 200,000 followers, and the "Secured Borders" Facebook group had over 130,000 followers.[61] According to Facebook, in total the IRA-controlled accounts made over 80,000 posts before their deactivation in August 2017, and these posts reached at least 29 million U.S persons and" may have reached an estimated 126 million people."[62]

4. U.S. Operations Through Twitter

A number of IRA employees assigned to the Translator Department served as Twitter specialists. [redacted][63]

The IRA's Twitter operations involved two strategies. First, IRA specialists operated certain Twitter accounts to create individual U.S. personas, [redacted][64] Separately, the IRA operated a network of automated Twitter accounts (commonly referred to as a bot network) that enabled the IRA to amplify existing content on Twitter.

a. Individualized Accounts

[redacted][65] [redacted][66] The IRA operated individualized Twitter accounts similar to the operation of its Facebook accounts, by continuously posting original content to

[60] 60
[61] 61
[62] 62
[63] 63
[64] 64
[65] 65
[66] 66

the accounts while also communicating with U.S. Twitter users directly (through public tweeting or Twitter's private messaging).

The IRA used many of these accounts to attempt to influence U.S. audiences on the election. Individualized accounts used to influence the U.S. presidential election included TEN_GOP (described above); jenn_abrams (claiming to be a Virginian Trump supporter with 70,000 followers); Pamela_Moore13 (claiming to be a Texan Trump supporter with 70,000 followers); and America_1st_ (an anti-immigration persona with 24,000 followers).[67] In May 2016, the IRA created the Twitter account march_for_trump, which promoted IRA-organized rallies in support of the Trump Campaign (described below).[68]

[redacted]

[redacted][69]

Using these accounts and others, the IRA provoked reactions from users and the media. Multiple IRA-posted tweets gained popularity.[70] U.S. media outlets also quoted tweets from IRA-controlled accounts and attributed them to the reactions of real U.S. persons.[71] Similarly, numerous high-profile U.S. persons, including former Ambassador Michael McFaul,[72] Roger Stone,[73] Sean Hannity,[74] and Michael Flynn Jr.,[75] retweeted or responded to tweets posted to

[67] 67
[68] 68
[69] 69
[70] 70
[71] 71
[72] 72
[73] 73
[74] 74
[75] 75

these IRA-controlled accounts. Multiple individuals affiliated with the Trump Campaign also promoted IRA tweets (discussed below).

b. IRA Botnet Activities [redacted][76]

[redacted][77]

[redacted][78]

In January 2018, Twitter publicly identified 3,814 Twitter accounts associated with the IRA.[79] According to Twitter, in the ten weeks before the 2016 U.S. presidential election, these accounts posted approximately 175,993 tweets, "approximately 8.4% of which were election-related."[80] Twitter also announced that it had notified approximately 1.4 million people who Twitter believed may have been in contact with an IRA-controlled account.[81]

5. U.S. Operations Involving Political Rallies

The IRA organized and promoted political rallies inside the United States while posing as U.S. grassroots activists. First, the IRA used one of its preexisting social media personas (Facebook groups and Twitter accounts, for example) to announce

[76] 76
[77] 77
[78] 78
[79] 79
[80] 80
[81] 81

and promote the event. The IRA then sent a large number of direct messages to followers of its social media account asking them to attend the event. From those who responded with interest in attending, the IRA then sought a U.S. person to serve as the event's coordinator. In most cases, the IRA account operator would tell the U.S. person that they personally could not attend the event due to some preexisting conflict or because they were somewhere else in the United States.[82] The IRA then further promoted the event by contacting U.S. media about the event and directing them to speak with the coordinator.[83] After the event, the IRA posted videos and photographs of the event to the IRA's social media accounts.[84]

The Office identified dozens of U.S. rallies organized by the IRA. The earliest evidence of a rally was a "confederate rally" in November 2015.[85] The IRA continued to organize rallies even after the 2016 U.S. presidential election. The attendance at rallies varied. Some rallies appear to have drawn few (if any) participants while others drew hundreds. The reach and success of these rallies was closely monitored [redacted]

From June 2016 until the end of the presidential campaign, almost all of the

[82] 82
[83] 83
[84] 84
[85] 85

U.S. rallies organized by the IRA focused on the U.S. election, often promoting the Trump Campaign and opposing the Clinton Campaign. Pro-Trump rallies included three in New York; a series of pro-Trump rallies in Florida in August 2016; and a series of pro-Trump rallies in October 2016 in Pennsylvania. The Florida rallies drew the attention of the Trump Campaign, which posted about the Miami rally on candidate Trump's Facebook account (as discussed below).[86]

Many of the same IRA employees who oversaw the IRA's social media accounts also conducted the day-to-day recruiting for political rallies inside the United States. [redacted].[87]

6. Targeting and Recruitment of U.S. Persons

As early as 2014, the IRA instructed its employees to target U.S. persons who could be used to advance its operational goals. Initially, recruitment focused on U.S. persons who could amplify the content posted by the IRA. [redacted].

[redacted].[88]

IRA employees frequently used [redacted] Twitter, Facebook, and Instagram to contact and recruit U.S. persons who followed the group. The IRA recruited U.S. persons from across the political spectrum. For example, the IRA targeted the family of [redacted] and a number of black social justice activists while posing as a grassroots group called "Black Matters US."[89] In February 2017, the persona "Black Fist" (purporting to want to teach African-Americans to protect themselves when contacted by law enforcement) hired a self-defense instructor in New York to offer classes sponsored by Black

[86] 86
[87] 87
[88] 88
[89] 89

Fist. The IRA also recruited moderators of conservative social media groups to promote IRA-generated content,[90] as well as recruited individuals to perform political acts (such as walking around New York City dressed up as Santa Claus with a Trump mask).[91]

[redacted].[92] [redacted].[93] [redacted].[94]

[redacted] as the IRA's online audience became larger, the IRA tracked U.S. persons with whom they communicated and had successfully tasked (with tasks ranging from organizing rallies to taking pictures with certain political messages). [redacted].[95]

[redacted]

[90] 90
[91] 91
[92] 92
[93] 93
[94] 94
[95] 95

7. Interactions and Contacts with the Trump Campaign

The investigation identified two different forms of connections between the IRA and . members of the Trump Campaign. (The investigation identified no similar connections between the IRA and the Clinton Campaign.) First, on multiple occasions, members and surrogates of the Trump Campaign promoted - typically by linking, retweeting, or similar methods of reposting - pro-Trump or anti-Clinton content published by the IRA through IRA-controlled social media accounts. Additionally, in a few instances, IRA employees represented themselves as U.S. persons to communicate with members of the Trump Campaign in an effort to seek assistance and coordination on IRA-organized political rallies inside the United States.

a. Trump Campaign Promotion of IRA Political Materials Among the U.S. "leaders of public opinion" targeted by the IRA were various members and surrogates of the Trump Campaign. In total, Trump Campaign affiliates promoted dozens of tweets, posts, and other political content created by the IRA.

- Posts from the IRA-controlled Twitter account TEN_GOP were cited or retweeted by multiple Trump Campaign officials and surrogates, including Donald J. Trump Jr.,[96] Eric Trump,[97] Kellyanne Conway,[98] Brad Parscale,[99] and Michael T. Flynn.[100] These posts included allegations of voter fraud,[101] as well as allegations that Secretary Clinton had mishandled classified information.[102]

- A November 7, 2016 post from the IRA-controlled Twitter account Pamela_Moore13 was retweeted by Donald J. Trump Jr.[103]

- On September 19, 2017, President Trump's personal account realDonaldTrump responded to a tweet from the IRA-controlled account

[96] 96
[97] 97
[98] 98
[99] 99
[100] 100
[101] 101
[102] 102
[103] 103

10_gop (the backup account of TEN_GOP, which had already been deactivated by Twitter). The tweet read: "We love you, Mr. President!"[104]

IRA employees monitored the reaction of the Trump Campaign and, later, Trump Administration officials to their tweets. For example, on August 23, 2016, the IRA-controlled persona "Matt Skiber" Facebook account sent a message to a U.S. Tea Party activist, writing that "Mr. Trump posted about our event in Miami! This is great!"[105] The IRA employee included a screenshot of candidate Trump's Facebook account, which included a post about the August 20, 2016 political rallies organized by the IRA.

[redacted].[106]

b. Contact with Trump Campaign Officials in Connection to Rallies
Starting in June 2016, the IRA contacted different U.S. persons affiliated with the Trump Campaign in an effort to coordinate pro-Trump IRA-organized rallies inside the United States. In all cases, the IRA contacted the Campaign while claiming to be U.S. political activists working on behalf of a conservative grassroots organization. The IRA's contacts included requests for signs and other materials to use at rallies,[107] as well as requests to promote the rallies and help coordinate logistics.[108] While certain campaign volunteers agreed to provide the requested support (for example, agreeing to set aside a number of signs), the investigation has not identified evidence that any Trump Campaign official understood the requests were coming from foreign nationals.

In sum, the investigation established that Russia interfered in the 2016 presidential election through the "active measures" social media campaign carried out by the IRA, an organization funded by Prigozhin and companies that he controlled. As explained further in Volume I, Section V.A, ***infra***, the Office

[104] 104
[105] 105
[106] 106
[107] 107
[108] 108

concluded (and a grand jury has alleged) that Prigozhin, his companies, and IRA employees violated U.S. law through these operations, principally by undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections.

III. Russian Hacking and Dumping Operations

Beginning in March 2016, units of the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) hacked the computers and email accounts of organizations, employees, and volunteers supporting the Clinton Campaign, including the email account of campaign chairman John Podesta. Starting in April 2016, the GRU hacked into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). The GRU targeted hundreds of email accounts used by Clinton Campaign employees, advisors, and volunteers. In total, the GRU stole hundreds of thousands of documents from the compromised email accounts and networks.[109] The GRU later released stolen Clinton Campaign and DNC documents through online personas, "DCLeaks" and "Guccifer 2.0," and later through the organization WikiLeaks. The release of the documents was designed and timed to interfere with the 2016 U.S. presidential election and undermine the Clinton Campaign.

The Trump Campaign showed interest in the WikiLeaks releases and, in the summer and fall of 2016, [redacted]. WikiLeaks's first Clinton-related release [redacted], the Trump Campaign stayed in contact [redacted] about WikiLeaks's activities. The investigation was unable to resolve [redacted]. WikiLeaks's release of the stolen Podesta emails on October 7, 2016, the same day a video from years earlier was published of Trump using graphic language about women.

A. GRU Hacking Directed at the Clinton Campaign

1. GRU Units Target the Clinton Campaign

Two military units of the GRU carried out the computer intrusions into the Clinton Campaign, DNC, and DCCC: Military Units 26165 and 74455.[110] Military Unit 26165 is a GRU cyber unit dedicated to targeting military, political, governmental, and non-governmental organizations outside of Russia, including in the United States.[111] The unit was sub-divided into departments with different specialties. One department, for example, developed specialized

[109] 109
[110] 110
[111] 111

malicious software "malware", while another department conducted large-scale spearphishing campaigns.[112] [redacted] a bitcoin mining operation to secure bitcoins used to purchase computer infrastructure used in hacking operations.[113]

Military Unit 74455 is a related GRU unit with multiple departments that engaged in cyber operations. Unit 74455 assisted in the release of documents stolen by Unit 26165, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU. Officers from Unit 74455 separately hacked computers belonging to state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.[114]

Beginning in mid-March 2016, Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as email accounts of individuals affiliated with the Clinton Campaign:[115]

- Unit 26165 used [redacted] to learn about [redacted] different Democratic websites, including democrats.org, hillaryclinton.com, dnc.org, and dccc.org. [redacted]. began before the GRU had obtained any credentials or gained access to these networks, indicating that the later DCCC and DNC intrusions were not crimes of opportunity but rather the result of targeting.[116]

- GRU officers also sent hundreds of spearphishing emails to the work and personal email accounts of Clinton Campaign employees and volunteers. Between March 10, 2016 and March 15, 2016, Unit 26165 appears to have sent approximately 90 spearphishing emails to email accounts at hillaryclinton.com. Starting on March 15, 2016, the GRU began targeting Google email accounts used by Clinton Campaign employees, along with a smaller number of dnc.org email accounts.[117]

The GRU spearphishing operation enabled it to gain access to numerous email accounts of Clinton Campaign employees and volunteers, including campaign

[112] 112
[113] 113
[114] 114
[115] 115
[116] 116
[117] 117

chairman John Podesta, junior volunteers assigned to the Clinton Campaign's advance team, informal Clinton Campaign advisors, and a DNC employee.[118] GRU officers stole tens of thousands of emails from spearphishing victims, including various Clinton Campaign-related communications.

2. Intrusions into the DCCC and DNC Networks

a. Initial Access By no later than April 12, 2016, the GRU had gained access to the DCCC computer network using the credentials stolen from a DCCC employee who had been successfully spearphished the week before. Over the ensuing weeks, the GRU traversed the network, identifying different computers connected to the DCCC network. By stealing network access credentials along the way (including those of IT administrators with unrestricted access to the system), the GRU compromised approximately 29 different computers on the DCCC network.[119]

Approximately six days after first hacking into the DCCC network, on April 18, 2016, GRU officers gained access to the DNC network via a virtual private network (VPN) connection[120] between the DCCC and DNC networks.[121] Between April 18, 2016 and June 8, 2016, Unit 26165 compromised more than 30 computers on the DNC network, including the DNC mail server and shared file server.[122]

b. Implantation of Malware on DCCC and DNC Networks Unit 26165 implanted on the DCCC and DNC networks two types of customized malware,[123] known as "X-Agent" and "X-Tunnel"; Mimikatz, a credential-harvesting tool; and rar.exe, a tool used in these intrusions to compile and compress materials for exfiltration. X-Agent was a multi-function hacking tool that allowed Unit 26165 to log keystrokes, take screenshots, and gather other data about the infected computers (e.g., file directories, operating systems).[124] X-Tunnel was a hacking tool that created an encrypted connection between the victim DCCC/DNC computers and GRU-controlled computers outside the DCCC and DNC networks that was capable of large-scale data transfers.[125] GRU officers then used X-Tunnel

[118] 118
[119] 119
[120] 120
[121] 121
[122] 122
[123] 123
[124] 124
[125] 125

to exfiltrate stolen data from the victim computers.

To operate X-Agent and X-Tunnel on the DCCC and DNC networks, Unit 26165 officers set up a group of computers outside those networks to communicate with the implanted malware.[126] The first set of GRU-controlled computers, known by the GRU as "middle servers," sent and received messages to and from malware on the DNC/DCCC networks. The middle servers, in turn, relayed messages to a second set of GRU-controlled computers, labeled internally by the GRU as an "AMS Panel." The AMS Panel [redacted] served as a nerve center through which GRU officers monitored and directed the malware's operations on the DNC/DCCC networks.[127]

The AMS Panel used to control X-Agent during the DCCC and DNC intrusions was housed on a leased computer located near [redacted] Arizona.[128] [redacted]

[redacted].[129]

[redacted]

[126] 126
[127] 127
[128] 128
[129] 129

The Arizona-based AMS Panel also stored thousands of files containing keylogging sessions captured through X-Agent. These sessions were captured as GRU officers monitored DCCC and DNC employees' work on infected computers regularly between April 2016 and June 2016. Data captured in these key logging sessions included passwords, internal communications between employees, banking information, and sensitive personal information.

c. Theft of Documents from DNC and DCCC Networks Officers from Unit 26165 stole thousands of documents from the DCCC and DNC networks, including significant amounts of data pertaining to the 2016 U.S. federal elections. Stolen documents included internal strategy documents, fundraising data, opposition research, and emails from the work inboxes of DNC employees.[130]

The GRU began stealing DCCC data shortly after it gained access to the network. On April 14, 2016 (approximately three days after the initial intrusion) GRU officers downloaded rar.exe onto the DCCC's document server. The following day, the GRU searched one compromised DCCC computer for files containing search terms that included "Hillary," "DNC," "Cruz," and "Trump."[131] On April 25, 2016, the GRU collected and compressed PDF and Microsoft documents from folders on the DCCC's shared file server that pertained to the 2016 election.[132] The GRU appears to have compressed and exfiltrated over 70 gigabytes of data from this file server.[133]

The GRU also stole documents from the DNC network shortly after gaining access. On April 22, 2016, the GRU copied files from the DNC network to GRU-controlled computers. Stolen documents included the DNC's opposition research into candidate Trump.[134] Between approximately May 25, 2016 and June 1, 2016, GRU officers accessed the DNC's mail server from a GRU-controlled computer leased inside the United States.[135] During these connections, Unit 26165 officers appear to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016.[136]

[130] 130
[131] 131
[132] 132
[133] 133
[134] 134
[135] 135
[136] 136

B. Dissemination of the Hacked Materials

The GRU's operations extended beyond stealing materials, and included releasing documents stolen from the Clinton Campaign and its supporters. The GRU carried out the anonymous release through two fictitious online personas that it created - DCLeaks and Guccifer 2.0 - and later through the organization WikiLeaks.

1. DCLeaks

The GRU began planning the releases at least as early as April 19, 2016, when Unit 26165 registered the domain dcleaks.com through a service that anonymized the registrant.[137] Unit 26165 paid for the registration using a pool of bitcoin that it had mined.[138] The dcleaks.com landing page pointed to different tranches of stolen documents, arranged by victim or subject matter. Other dcleaks.com pages contained indexes of the stolen emails that were being released (bearing the sender, recipient, and date of the email). To control access and the timing of releases, pages were sometimes password-protected for a period of time and later made unrestricted to the public.

Starting in June 2016, the GRU posted stolen documents onto the website dcleaks.com, including documents stolen from a number of individuals associated with the Clinton Campaign. These documents appeared to have originated from personal email accounts (in particular, Google and Microsoft accounts), rather than the DNC and DCCC computer networks. DCLeaks victims included an advisor to the Clinton Campaign, a former DNC employee and Clinton Campaign employee, and four other campaign volunteers.[139] The GRU released through dcleaks.com thousands of documents, including personal identifying and financial information, internal correspondence related to the Clinton Campaign and prior political jobs, and fundraising files and information.[140]

GRU officers operated a Facebook page under the DCLeaks moniker, which they primarily used to promote releases of materials.[141] The Facebook page was administered through a small number of preexisting GRU-controlled Facebook accounts.[142]

---

[137] 137
[138] 138
[139] 139
[140] 140
[141] 141
[142] 142

GRU officers also used the DCLeaks Facebook account, the Twitter account dcleaks_, and the email account dcleaksprojectgmail.com to communicate privately with reporters and other U.S. persons. GRU officers using the DCLeaks persona gave certain reporters early access to archives of leaked files by sending them links and passwords to pages on the dcleaks.com website that had not yet become public. For example, on July 14, 2016, GRU officers operating under the DCLeaks persona sent a link and password for a non-public DCLeaks webpage to a U.S. reporter via the Facebook account.[143] Similarly, on September 14, 2016, GRU officers sent reporters Twitter direct messages from dcleaks_, with a password to another non-public part of the dcleaks.com website.[144]

The DCLeaks.com website remained operational and public until March 2017.

2. Guccifer 2.0

On June 14, 2016, the DNC and its cyber-response team announced the breach of the DNC network and suspected theft of DNC documents. In the statements, the cyber-response team alleged that Russian state-sponsored actors (which they referred to as "Fancy Bear") were responsible for the breach.[145] Apparently in response to that announcement, on June 15, 2016, GRU officers using the persona Guccifer 2.0 created a WordPress blog. In the hours leading up to the launch of that WordPress blog, GRU officers logged into a Moscow-based server used and managed by Unit 74455 and searched for a number of specific words and phrases in English, including "some hundred sheets," "illuminati," and "worldwide known." Approximately two hours after the last of those searches, Guccifer 2.0 published its first post, attributing the DNC server hack to a lone Romanian hacker and using several of the unique English words and phrases that the GRU officers had searched for that day.[146]

That same day, June 15, 2016, the GRU also used the Guccifer 2.0 WordPress blog to begin releasing to the public documents stolen from the DNC and DCCC computer networks. The Guccifer 2.0 persona ultimately released thousands of documents stolen from the DNC and DCCC in a series of blog posts between June 15, 2016 and October 18, 2016.[147] Released documents included opposition research performed by the DNC (including a memorandum analyzing

[143] 143
[144] 144
[145] 145
[146] 146
[147] 147

potential criticisms of candidate Trump), internal policy documents (such as recommendations on how to address politically sensitive issues), analyses of specific congressional races, and fundraising documents. Releases were organized around thematic issues, such as specific states (e.g., Florida and Pennsylvania) that were perceived as competitive in the 2016 U.S. presidential election.

Beginning in late June 2016, the GRU also used the Guccifer 2.0 persona to release documents directly to reporters and other interested individuals. Specifically, on June 27, 2016, Guccifer 2.0 sent an email to the news outlet The Smoking Gun offering to provide "exclusive access to some leaked emails linked [to] Hillary Clinton's staff."[148] The GRU later sent the reporter a password and link to a locked portion of the dcleaks.com website that contained an archive of emails stolen by Unit 26165 from a Clinton Campaign volunteer in March 2016.[149] That the Guccifer 2.0 persona provided reporters access to a restricted portion of the DCLeaks website tends to indicate that both personas were operated by the same or a closely-related group of people.[150]

The GRU continued its release efforts through Guccifer 2.0 into August 2016. For example, on August 15, 2016, the Guccifer 2.0 persona sent a candidate for the U.S. Congress documents related to the candidate's opponent.[151] On August 22, 2016, the Guccifer 2.0 persona transferred approximately 2.5 gigabytes of Florida-related data stolen from the DCCC to a U.S. blogger covering Florida politics.[152] On August 22, 2016, the Guccifer 2.0 persona sent a U.S. reporter documents stolen from the DCCC pertaining to the Black Lives Matter movement.[153]

The GRU was also in contact through the Guccifer 2.0 persona with [redacted] a former Trump Campaign member [redacted].[154] In early August 2016, [redacted] Twitter's suspension of the Guccifer 2.0 Twitter account. After it was reinstated, GRU officers posing as Guccifer 2.0 wrote [redacted] a private message, "thank u for writing back ... do u find anyt[h]ing interesting in the docs

[148] 148
[149] 149
[150] 150
[151] 151
[152] 152
[153] 153
[154] 154

i posted?" On August 17, 2016, the GRU added, "please tell me if i can help u anyhow ... it would be a great pleasure to me." On September 9, 2016, the GRU - again posing as Guccifer 2.0 - referred to a stolen DCCC document posted online and asked [redacted] "what do u think of the info on the turnout model for the democrats entire presidential campaign." [redacted] responded, "pretty standard."[155] The investigation did not identify evidence of other communications between [redacted] and Guccifer 2.0.

3. Use of WikiLeaks

In order to expand its interference in the 2016 U.S. presidential election, the GRU units transferred many of the documents they stole from the DNC and the chairman of the Clinton Campaign to WikiLeaks. GRU officers used both the DCLeaks and Guccifer 2.0 personas to communicate with WikiLeaks through Twitter private messaging and through encrypted channels, including possibly through WikiLeaks's private communication system.

a. WikiLeaks's Expressed Opposition Toward the Clinton Campaign

WikiLeaks, and particularly its founder Julian Assange, privately expressed opposition to candidate Clinton well before the first release of stolen documents. In November 2015, Assange wrote to other members and associates of WikiLeaks that "[w]e believe it would be much better for GOP to win... Dems+Media+liberals woudl [sic] then form a block to reign in their worst qualities.... With Hillary in charge, GOP will be pushing for her worst qualities., dems+media+neoliberals will be mute.... She's a bright, well connected, sadisitic sociopath."[156]

In March 2016, WikiLeaks released a searchable archive of approximately 30,000 Clinton emails that had been obtained through FOIA litigation.[157] While designing the archive, one WikiLeaks member explained the reason for building the archive to another associate:

> [W]e want this repository to become "the place" to search for background on hillary's plotting at the state department during 2009-2013.... Firstly because its useful and will annoy Hillary, but secondly because we want to be seen to be a resource/player in the

[155] 155
[156] 156
[157] 157

> US election, because eit [sic] may en[]courage people to send us even more important leaks.[158]

b. WikiLeaks's First Contact with Guccifer 2.0 and DCLeaks Shortly after the GRU's first release of stolen documents through dcleaks.com in June 2016, GRU officers also used the DCLeaks persona to contact WikiLeaks about possible coordination in the future release of stolen emails. On June 14, 2016, dcleaks_ sent a direct message to WikiLeaks, noting, "You announced your organization was preparing to publish more Hillary's emails. We are ready to support you. We have some sensitive information too, in particular, her financial documents. Let's do it together. What do you think about publishing our info at the same moment? Thank you."[159] [redacted].

Around the same time, WikiLeaks initiated communications with the GRU persona Guccifer 2.0 shortly after it was used to release documents stolen from the DNC. On June 22, 2016, seven days after Guccifer 2.0's first releases of stolen DNC documents, WikiLeaks used Twitter's direct message function to contact the Guccifer 2.0 Twitter account and suggest that Guccifer 2.0 "[s]end any new material [stolen from the DNC] here for us to review and it will have a much higher impact than what you are doing."[160]

On July 6, 2016, WikiLeaks again contacted Guccifer 2.0 through Twitter's private messaging function, writing, "if you have anything hillary related we want it in the next tweo [sic] days prefable [sic] because the DNC is approaching and she will solidify bernie supporters behind her after." The Guccifer 2.0 persona responded, "ok ... i see." WikiLeaks also explained, "we think trump has only a 25% chance of winning against hillary ... so conflict between bernie and hillary is interesting."[161]

c. The GRU's Transfer of Stolen Materials to WikiLeaks Both the GRU and WikiLeaks sought to hide their communications, which has limited the Office's ability to collect all of the communications between them. Thus, although it is clear that the stolen DNC and Podesta documents were transferred from the GRU

[158] 158
[159] 159
[160] 160
[161] 161

to WikiLeaks, [redacted].

The Office was able to identify when the GRU (operating through its personas Guccifer 2.0 and DCLeaks) transferred some of the stolen documents to WikiLeaks through online archives set up by the GRU. Assange had access to the internet from the Ecuadorian Embassy in London, England. [redacted][162]

On July 14, 2016, GRU officers used a Guccifer 2.0 email account to send WikiLeaks an email bearing the subject "big archive" and the message "a new attempt."[163] The email contained an encrypted attachment with the name "wk dnc link1.txt.gpg."[164] Using the Guccifer 2.0 Twitter account, GRU officers sent WikiLeaks an encrypted file and instructions on how to open it.[165] On July 18, 2016, WikiLeaks confirmed in a direct message to the Guccifer 2.0 account that it had "the 1 Gb or so archive" and would make a release of the stolen documents "this week."[166] On July 22, 2016, WikiLeaks released over 20,000 emails and other documents stolen from the DNC computer networks.[167] The Democratic National Convention began three days later.

Similar communications occurred between WikiLeaks and the GRU-operated persona DCLeaks. On September 15, 2016, dcleaks wrote to WikiLeaks, "hi there! I'm from DC Leaks. How could we discuss some submission-related issues? Am trying to reach out to you via your secured chat but getting no response. I've got something that might interest you. You won't be disappointed, I promise."[168] The WikiLeaks account responded, "Hi there," without further elaboration. The dcleaks_ account did not respond immediately.

The same day, the Twitter account guccifer_2 sent dcleaks_ a direct message, which is the first known contact between the personas.[169] During subsequent communications, the Guccifer 2.0 persona informed DCLeaks that WikiLeaks was trying to contact DCLeaks and arrange for a way to speak through encrypted

[162] 162
[163] 163
[164] 164
[165] 165
[166] 166
[167] 167
[168] 168
[169] 169

emails.[170]

An analysis of the metadata collected from the WikiLeaks site revealed that the stolen Podesta emails show a creation date of September 19, 2016.[171] Based on information about Assange's computer and its possible operating system, this date may be when the GRU staged the stolen Podesta emails for transfer to WikiLeaks (as the GRU had previously done in July 2016 for the DNC emails).[172] The WikiLeaks site also released PDFs and other documents taken from Podesta that were attachments to emails in his account; these documents had a creation date of October 2, 2016, which appears to be the date the attachments were separately staged by WikiLeaks on its site.[173]

Beginning on September 20, 2016, WikiLeaks and DCLeaks resumed communications in a brief exchange. On September 22, 2016, a DCLeaks email account dcleaksprojectgmail.com sent an email to a WikiLeaks account with the subject "Submission" and the message "Hi from DCLeaks." The email contained a PGP-encrypted message with the filename "wiki_mail.txt.gpg."[174] [redacted] The email, however, bears a number of similarities to the July 14, 2016 email in which GRU officers used the Guccifer 2.0 persona to give WikiLeaks access to the archive of DNC files. On September 22, 2016 (the same day of DCLeaks' email to WikiLeaks), the Twitter account dcleaks sent a single message to WikiLeaks with the string of characters [redacted].

The Office cannot rule out that stolen documents were transferred to WikiLeaks through intermediaries who visited during the summer of 2016. For example, public reporting identified Andrew Müller-Maguhn as a WikiLeaks associate who may have assisted with the transfer of these stolen documents to WikiLeaks.[175] [redacted].[176]

On October 7, 2016, WikiLeaks released the first emails stolen from the

[170] 170
[171] 171
[172] 172
[173] 173
[174] 174
[175] 175
[176] 176

Podesta email account. In total, WikiLeaks released 33 tranches of stolen emails between October 7, 2016 and November 7, 2016. The releases included private speeches given by Clinton;[177] internal communications between Podesta and other high-ranking members of the Clinton Campaign;[178] and correspondence related to the Clinton Foundation.[179] In total, WikiLeaks released over 50,000 documents stolen from Podesta' s personal email account. The last-in-time email released from Podesta's account was dated March 21, 2016, two days after Podesta received a spearphishing email sent by the GRU.

d. WikiLeaks Statements Dissembling About the Source of Stolen Materials As reports attributing the DNC and DCCC hacks to the Russian government emerged, WikiLeaks and Assange made several public statements apparently designed to obscure the source of the materials that WikiLeaks was releasing. The file-transfer evidence described above and other information uncovered during the investigation discredit WikiLeaks's claims about the source of material that it posted.

Beginning in the summer of 2016, Assange and WikiLeaks made a number of statements about Seth Rich, a former DNC staff member who was killed in July 2016. The statements about Rich implied falsely that he had been the source of the stolen DNC emails. On August 9, 2016, the @WikiLeaks Twitter account posted: "ANNOUNCE: WikiLeaks has decided to issue a US$20k reward for information leading to conviction for the murder of DNC staffer Seth Rich."[180] Likewise, on August 25, 2016, Assange was asked in an interview, "Why are you so interested in Seth Rich's killer?" and responded, "We're very interested in anything that might be a threat to alleged Wikileaks sources." The interviewer responded to Assange's statement by commenting, "I know you don't want to reveal your source, but it certainly sounds like you're suggesting a man who leaked information to WikiLeaks was then murdered." Assange replied, "If there's someone who's potentially connected to our publication, and that person has been murdered in suspicious circumstances, it doesn't necessarily mean that the two are connected. But it is a very serious matter ... that type of allegation is very serious, as it's taken very seriously by us."[181]

[177] 177
[178] 178
[179] 179
[180] 180
[181] 181

After the U.S. intelligence community publicly announced its assessment that Russia was behind the hacking operation, Assange continued to deny that the Clinton materials released by WikiLeaks had come from Russian hacking. According to media reports, Assange told a U.S. congressman that the DNC hack was an "inside job," and purported to have "physical proof' that Russians did not give materials to Assange.[182]

4. Additional GRU Cyber Operations

While releasing the stolen emails and documents through DCLeaks, Guccifer 2.0, and WikiLeaks, GRU officers continued to target and hack victims linked to the Democratic campaign and, eventually, to target entities responsible for election administration in several states.

a. Summer and Fall 2016 Operations Targeting Democrat-Linked Victims

On July 27 2016, Unit 26165 targeted email accounts connected to candidate Clinton's personal office [redacted]. Earlier that day, candidate Trump made public statements that included the following: "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing. I think you will probably be rewarded mightily by our press."[183] The "30,000 emails" were apparently a reference to emails described in media accounts as having been stored on a personal server that candidate Clinton had used while serving as Secretary of State.

Within approximately five hours of Trump's statement, GRU officers targeted for the first time Clinton's personal office. After candidate Trump's remarks, Unit 26165 created and sent malicious links targeting 15 email accounts at the domain [redacted] including an email account belonging to Clinton aide [redacted]. The investigation did not find evidence of earlier GRU attempts to compromise accounts hosted on this domain. It is unclear how the GRU was able to identify these email accounts, which were not public.[184]

Unit 26165 officers also hacked into a DNC account hosted on a cloud-computing service [redacted]. On September 20, 2016, the GRU began to generate copies of the DNC data [redacted] function designed to allow users to produce backups of databases (referred to [redacted] as "snapshots"). The GRU then stole those snapshots by moving them to [redacted]

[182] 182
[183] 183
[184] 184

[redacted] account that they controlled; from there, the copies were moved to GRU-controlled computers. The GRU stole approximately 300 gigabytes of data from the DNC cloud-based account.[185]

5. Intrusions Targeting the Administration of U.S. Elections

In addition to targeting individuals involved in the Clinton Campaign, GRU officers also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities.[186] The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations.[187] The GRU continued to target these victims through the elections in November 2016. While the investigation identified evidence that the GRU targeted these individuals and entities, the Office did not investigate further. The Office did not, for instance, obtain or examine servers or other relevant items belonging to these victims. The Office understands that the FBI, the U.S. Department of Homeland Security, and the states have separately investigated that activity.

By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents).[188] In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters,[189] and extracted data related to thousands of U.S. voters before the malicious activity was identified.[190]

GRU officers [redacted] scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers

[185] 185
[186] 186
[187] 187
[188] 188
[189] 189
[190] 190

[redacted] for vulnerabilities on websites of more than two dozen states. [redacted]. Similar [redacted] for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of [redacted], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.[191] The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer.[192] The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

C. Trump Campaign and the Dissemination of Hacked Materials

The Trump Campaign showed interest in WikiLeaks's releases of hacked materials throughout the summer and fall of 2016. [redacted].

1. [redacted] Harm to Ongoing Matter

a. Background

[redacted].

[191] 191
[192] 192

b. Contacts with the Campaign about WikiLeaks [redacted].[193] [redacted]. On June 12, 2016, Assange claimed in a televised interview to "have emails relating to Hillary Clinton which are pending publication,"[194] but provided no additional context.

In debriefings with the Office, former campaign chairman Rick Gates said that, [redacted].[195] [redacted]. Gates recalled candidate Trump being generally frustrated that the Clinton emails had not been found.[196]

Paul Manafort, who would later become campaign chairman, [redacted].[197] [redacted].[198]

[193] 193
[194] 194
[195] 195
[196] 196
[197] 197
[198] 198