

# Open Source Edition of the 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://iandennismiller.github.io/mueller-report/>

Status: in progress

# Table of Contents - Volume I

Introduction to Volume I . . . . .	1
Executive Summary to Volume I . . . . .	4
<b>I. The Special Counsel’s Investigation . . . . .</b>	<b>14</b>
<b>II. Russian “Active Measures” Social Media Campaign . . . . .</b>	<b>19</b>
A. Structure of the Internet Research Agency . . . . .	20
B. Funding and Oversight from Concord and Prigozhin . . . . .	22
C. The IRA Targets U.S. Elections . . . . .	24
1. The IRA Ramps Up U.S. Operations as Early as 2014 . . . . .	24
2. U.S. Operations Through IRA-Controlled Social Media Accounts . . . . .	26
3. U.S. Operations Through Facebook . . . . .	28
4. U.S. Operations Through Twitter . . . . .	30
a. Individualized Accounts . . . . .	30
b. IRA Botnet Activities . . . . .	31
5. U.S. Operations Involving Political Rallies . . . . .	32
6. Targeting and Recruitment of U.S. Persons . . . . .	34
7. Interactions and Contacts with the Trump Campaign . . . . .	36
a. Trump Campaign Promotion of IRA Political Materials . . . . .	36
b. Contact with Trump Campaign Officials in Connection to Rallies . . . . .	37
<b>III. Russian Hacking and Dumping Operations . . . . .</b>	<b>39</b>
A. GRU Hacking Directed at the Clinton Campaign . . . . .	39
1. GRU Units Target the Clinton Campaign . . . . .	39
2. Intrusions into the DCCC and DNC Networks . . . . .	41
a. Initial Access . . . . .	41
b. Implantation of Malware on DCCC and DNC Networks . . . . .	41
c. Theft of Documents from DNC and DCCC Networks . . . . .	43
B. Dissemination of the Hacked Materials . . . . .	44
1. DCLeaks . . . . .	44

## TABLE OF CONTENTS - VOLUME I

2.	Guccifer 2.0 . . . . .	46
3.	Use of WikiLeaks . . . . .	48
a.	WikiLeaks's Expressed Opposition Toward the Clinton Campaign . . . . .	48
b.	WikiLeaks's First Contact with Guccifer 2.0 and DCLeaks . . . . .	48
c.	The GRU's Transfer of Stolen Materials to WikiLeaks . . . . .	49
d.	WikiLeaks Statements Dissembling About the Source of Stolen Materials . . . . .	52
4.	Additional GRU Cyber Operations . . . . .	53
a.	Summer and Fall 2016 Operations Targeting Democrat-Linked Victims . . . . .	53
5.	Intrusions Targeting the Administration of U.S. Elections	54
C.	Trump Campaign and the Dissemination of Hacked Materials	55
1.	[Harm to Ongoing Matter] . . . . .	55
a.	Background . . . . .	55
b.	Contacts with the Campaign about WikiLeaks	56
c.	[ : Harm to Ongoing Matter] . . . . .	58
d.	WikiLeaks's October 7, 2016 Release of Stolen Podesta Emails . . . . .	61
e.	Donald Trump Jr. Interaction with WikiLeaks	62
2.	Other Potential Campaign Interest in Russian Hacked Materials . . . . .	64
a.	Henry Oknyansky (a/k/a Henry Greenberg) .	64
b.	Campaign Efforts to Obtain Deleted Clinton Emails . . . . .	65

<b>IV.</b>	<b>Russian Government Links to and Contacts with The Trump Campaign . . . . .</b>	<b>70</b>
A.	Campaign Period (September 2015 - November 8, 2016) . . .	70
1.	Trump Tower Moscow Project . . . . .	70
a.	Trump Tower Moscow Venture with the Crocus Group (2013-2014) . . . . .	70
b.	Communications with I.C. Expert Investment Company and Giorgi Rtskhiladze (Summer and Fall 2015) . . . . .	70

## TABLE OF CONTENTS - VOLUME I

c.	Letter of Intent and Contacts to Russian Government (October 2015-January 2016) . . . . .	70
i.	Trump Signs the Letter of Intent on behalf of the Trump Organization . . . . .	70
ii.	Post-LOI Contacts with Individuals in Russia . . . . .	70
d.	Discussions about Russia Travel by Michael Cohen or Candidate Trump (December 2015-June 2016) . . . . .	70
i.	Sater's Overtures to Cohen to Travel to Russia . . . . .	70
ii.	Candidate Trump's Opportunities to Travel to Russia . . . . .	70
2.	George Papadopoulos . . . . .	70
a.	Origins of Campaign Work . . . . .	70
b.	Initial Russia-Related Contacts . . . . .	70
c.	March 31 Foreign Policy Team Meeting . . . . .	70
d.	George Papadopoulos Learns That Russia Has "Dirt" in the Form of Clinton Emails . . . . .	71
e.	Russia-Related Communications With The Campaign . . . . .	71
f.	Trump Campaign Knowledge of "Dirt" . . . . .	71
g.	Additional George Papadopoulos Contact . . . . .	71
3.	Carter Page . . . . .	71
a.	Background . . . . .	71
b.	Origins of and Early Campaign Work . . . . .	71
c.	Carter Page's July 2016 Trip To Moscow . . . . .	71
d.	Later Campaign Work and Removal from the Campaign . . . . .	71
4.	Dimitri Simes and the Center for the National Interest . . . . .	71
a.	CNI and Dimitri Simes Connect with the Trump Campaign . . . . .	71
b.	National Interest Hosts a Foreign Policy Speech at the Mayflower Hotel . . . . .	71
c.	Jeff Sessions's Post-Speech Interactions with CNI . . . . .	71
d.	Jared Kushner's Continuing Contacts with Simes . . . . .	71

## TABLE OF CONTENTS - VOLUME I

5.	June 9, 2016 Meeting at Trump Tower . . . . .	71
a.	Setting Up the June 9 Meeting . . . . .	71
i.	Outreach to Donald Trump Jr . . . . .	71
ii.	Awareness of the Meeting Within the Campaign . . . . .	71
b.	The Events of June 9, 2016 . . . . .	72
i.	Arrangements for the Meeting . . . . .	72
ii.	Conduct of the Meeting . . . . .	72
c.	Post-June 9 Events . . . . .	72
6.	Events at the Republican National Convention . . . . .	72
a.	Ambassador Kislyak's Encounters with Senator Sessions and J.D. Gordon the Week of the RNC . . . . .	72
b.	Change to Republican Party Platform . . . . .	72
7.	Post-Convention Contacts with Kislyak . . . . .	72
a.	Ambassador Kislyak Invites J.D. Gordon to Breakfast at the Ambassador's Residence . . . . .	72
b.	Senator Sessions's September 2016 Meeting with Ambassador Kislyak . . . . .	72
8.	Paul Manafort . . . . .	72
a.	Paul Manafort's Ties to Russia and Ukraine . . . . .	72
i.	Oleg Deripaska Consulting Work . . . . .	72
ii.	Political Consulting Work . . . . .	72
iii.	Konstantin Kilimnik . . . . .	72
b.	Contacts during Paul Manafort's Time with the Trump Campaign . . . . .	72
i.	Paul Manafort Joins the Campaign . . . . .	72
ii.	Paul Manafort's Campaign-Period Contacts . . . . .	73
iii.	Paul Manafort's Two Campaign-Period Meetings with Konstantin Kilimnik in the United States . . . . .	73
c.	Post-Resignation Activities . . . . .	73
B.	Post-Election and Transition-Period Contacts . . . . .	73
1.	Immediate Post-Election Activity . . . . .	73
a.	Outreach from the Russian Government . . . . .	73
b.	High-Level Encouragement of Contacts through Alternative Channels . . . . .	73

## TABLE OF CONTENTS - VOLUME I

2.	Kirill Dmitriev’s Transition-Era Outreach to the Incoming Administration . . . . .	73
a.	Background . . . . .	73
b.	Kirill Dmitriev’s Post-Election Contacts With the Incoming Administration . . . . .	73
c.	Erik Prince and Kirill Dmitriev Meet in the Seychelles . . . . .	73
i.	George Nader and Erik Prince Arrange Seychelles Meeting with Dmitriev . . . . .	73
ii.	The Seychelles Meetings . . . . .	73
iii.	Erik Prince’s Meeting with Steve Bannon after the Seychelles Trip . . . . .	73
d.	Kirill Dmitriev’s Post-Election Contact with Rick Gerson Regarding U.S.-Russia Relations . . . . .	73
3.	Ambassador Kislyak’s Meeting with Jared Kushner and Michael Flynn in Trump Tower Following the Election . . . . .	74
4.	Jared Kushner’s Meeting with Sergey Gorkov . . . . .	74
5.	Petr Aven’s Outreach Efforts to the Transition Team . . . . .	74
6.	Carter Page Contact with Deputy Prime Minister Arkady Dvorkovich . . . . .	74
7.	Contacts With and Through Michael T. Flynn . . . . .	74
a.	United Nations Vote on Israeli Settlements . . . . .	74
b.	U.S. Sanctions Against Russia . . . . .	74
<b>V.</b>	<b>Prosecution and Declination Decisions . . . . .</b>	<b>75</b>
A.	Russian ”Active Measures” Social Media Campaign . . . . .	75
B.	Russian Hacking and Dumping Operations . . . . .	75
1.	Section 1030 Computer-Intrusion Conspiracy . . . . .	75
a.	Background . . . . .	75
b.	Charging Decision As to [ : Harm to Ongoing Matter] . . . . .	75
2.	Potential Section 1030 Violation By [ : Personal Privacy] . . . . .	75
C.	Russian Government Outreach and Contacts . . . . .	75
1.	Potential Coordination: Conspiracy and Collusion . . . . .	75
2.	Potential Coordination: Foreign Agent Statutes (FARA and 18 U.S.C. § 951) . . . . .	75
a.	Governing Law . . . . .	75

## TABLE OF CONTENTS - VOLUME I

	b.	Application . . . . .	75
3.		Campaign Finance . . . . .	75
	a.	Overview Of Governing Law . . . . .	75
	b.	Application to June 9 Trump Tower Meeting . . . . .	75
	i.	Thing-of-Value Element . . . . .	75
	ii.	Willfulness . . . . .	75
	iii.	Difficulties in Valuing Promised Information . . . . .	75
	c.	Application to WikiLeaks [ : HOM] . . . . .	75
	i.	Questions Over [ : Harm to Ongoing Matter] . . . . .	76
	ii.	Willfulness . . . . .	76
	iii.	Constitutional Considerations . . . . .	76
	iv.	Analysis [ : HOM] . . . . .	76
4.		False Statements and Obstruction of the Investigation . . . . .	76
	a.	Overview Of Governing Law . . . . .	76
	b.	Application to Certain Individuals . . . . .	76
	i.	George Papadopoulos . . . . .	76
	ii.	[ : Personal Privacy] . . . . .	76
	iii.	Michael Flynn . . . . .	76
	iv.	Michael Cohen . . . . .	76
	v.	[ : HOM] . . . . .	76
	vi.	Jeff Sessions . . . . .	76
	vii.	Others Interviewed During the Investigation . . . . .	76

## 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



## Introduction to Volume I

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

## Introduction to Volume I

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] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[illegible]

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.

# Executive Summary to Volume I

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.

[illegible]

## 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

## Executive Summary to Volume I

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.

## Executive Summary to Volume I

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

## Executive Summary to Volume I

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.



## Executive Summary to Volume I

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 Comey 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, Comey 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.



## Executive Summary to Volume I

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

## Executive Summary to Volume I

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.).

(b) (7)(C), (b) (7)(D). The information requested is withheld because it is confidential under FOIA exemption (b) (7)(C) and (b) (7)(D).

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 guilty to making false statements to Congress about the Trump Moscow project. [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [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 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 Department 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.

12

## Executive Summary to Volume I

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.

Open Source Draft

## I. THE SPECIAL COUNSEL'S INVESTIGATION

### 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. Comey 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

## I. THE SPECIAL COUNSEL'S INVESTIGATION

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, ██████████ Roger Stone, and ██████████” ”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,

## I. THE SPECIAL COUNSEL'S INVESTIGATION

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.

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.

## I. THE SPECIAL COUNSEL'S INVESTIGATION

---

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.<sup>1</sup>

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

---

<sup>1</sup>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.



## I. THE SPECIAL COUNSEL'S INVESTIGATION

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 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.

Open Source Draft

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

### 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”).<sup>2</sup> The IRA conducted social media operations targeted at large U.S. audiences with the goal of sowing discord in the U.S. political system.<sup>3</sup> These operations constituted “active measures” ( ), a term that typically refers to operations conducted by Russian security services aimed at influencing the course of international affairs.<sup>4</sup>

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

---

<sup>2</sup>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.

<sup>3</sup> [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.

<sup>4</sup>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”).

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

in the names of U.S. persons and entities. Some IRA employees, posing as U.S. persons and without revealing their Russian 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.<sup>5</sup> 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 Facebook accounts.<sup>6</sup> 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.<sup>7</sup>

### A. Structure of the Internet Research Agency

[illegible]

<sup>5</sup>Internet Research Agency Indictment §§52, 54, 55(a), 56, 74; [REDACTED]

<sup>6</sup>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.

<sup>7</sup>Twitter, Update on Twitter’s Review of the 2016 US Election (Jan. 31, 2018).

<sup>8</sup>See SM-2230634, serial 92.

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

The organization quickly grew. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]<sup>11</sup> [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED]<sup>12</sup>

[illegible][illegible][illegible]

9

<sup>11</sup>See SM-2230634, serial 86 [REDACTED]

12

13

<sup>14</sup>See, e.g., SM-2230634, serials 9, 113 & 180 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

15

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

[REDACTED] 16

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

[REDACTED] Prigozhin was sanctioned by the U.S. Treasury Department in December 2016,<sup>19</sup> [REDACTED] 20

[REDACTED] 21 Numerous media sources have reported on Prigozhin’s ties to Putin, and the two have appeared together in public photographs.<sup>22</sup>

[REDACTED] 23

<sup>16</sup> [REDACTED]. See SM-2230634, serials 131 & 204.

<sup>17</sup> [REDACTED]

<sup>18</sup> [REDACTED]

<sup>19</sup>U.S. Treasury Department, “Treasury Sanctions Individuals and Entities in Connection with Russia’s Occupation of Crimea and the Conflict in Ukraine” (Dec. 20, 2016).

<sup>20</sup> [REDACTED]

<sup>21</sup> [REDACTED]

<sup>22</sup>See, e.g., Neil MacFarquhar, Yevgeny Prigozhin, Russian Oligarch Indicted by US., Is Known as “Putin’s Cook”, New York Times (Feb. 16, 2018).

<sup>23</sup> [REDACTED]



## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

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).<sup>31</sup> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[illegible]

### C. The IRA Targets U.S. Elections

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

[illegible]

[REDACTED] [REDACTED]  
[REDACTED] [REDACTED] 33 [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] 34  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED]. [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED]

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

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

3333

3434





## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

[illegible]

## 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."<sup>42</sup> Starting as early as 2014, the IRA's U.S. operations included social media specialists focusing on Facebook, YouTube, and Twitter.<sup>43</sup> The IRA later added specialists who operated on Tumblr and Instagram accounts.<sup>44</sup>

Initially, the IRA created social media accounts that pretended to be the personal accounts of U.S. persons.<sup>45</sup> 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.<sup>46</sup> 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.

[illegible]

4141

4242

4343

4444

4545

4646

47 47

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

48

[illegible]

The focus on the U.S. presidential campaign continued through 2016. In █████ 2016 internal █████ 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.”<sup>51</sup>

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

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]. [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED].

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED].

52

4848

4949

5050

5151

5252

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

### 3. U.S. Operations Through Facebook

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

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

i [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

ii [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

iii [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]<sup>53</sup>

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]<sup>54</sup>

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.”<sup>55</sup>

To reach larger U.S. audiences, the IRA purchased advertisements from Facebook that promoted the IRA groups on the newsfeeds of U.S.

---

<sup>53</sup>53

<sup>54</sup>54

<sup>55</sup>55

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

audience members. According to Facebook, the IRA purchased over 3,500 advertisements, and the expenditures totaled approximately \$100,000.<sup>56</sup>

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.”<sup>57</sup> 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.”<sup>58</sup> IRA-purchased advertisements featuring Clinton were, with very few exceptions, negative.<sup>59</sup>

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 hashtag “#KIDS4TRUMP.”<sup>60</sup> 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.<sup>61</sup> According to Facebook, in total the IRA-controlled accounts made over 80,000 posts before their deactivation in August 2017,

---

<sup>56</sup>56

<sup>57</sup>57

<sup>58</sup>58

<sup>59</sup>59

<sup>60</sup>60

<sup>61</sup>61

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

and these posts reached at least 29 million U.S. persons and” may have reached an estimated 126 million people.”<sup>62</sup>

#### 4. U.S. Operations Through Twitter

The IRA's Twitter operations involved two strategies. First, IRA specialists operated certain Twitter accounts to create individual U.S. personas, [REDACTED] [REDACTED]<sup>63</sup>

[REDACTED]

[REDACTED]<sup>64</sup> 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]<sup>65</sup>

[REDACTED]

[REDACTED]<sup>66</sup> The IRA operated individualized Twitter accounts similar to the operation of its Facebook accounts, by continuously posting original content to 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).<sup>67</sup> 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).<sup>68</sup>

6262

6363

6464

6565

6666

6767

6868

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

[REDACTED]

[REDACTED]

Using these accounts and others, the IRA provoked reactions from users and the media. Multiple IRA-posted tweets gained popularity.<sup>70</sup> U.S. media outlets also quoted tweets from IRA-controlled accounts and attributed them to the reactions of real U.S. persons.<sup>71</sup> Similarly, numerous high-profile U.S. persons, including former Ambassador Michael McFaul,<sup>72</sup> Roger Stone,<sup>73</sup> Sean Hannity,<sup>74</sup> and Michael Flynn Jr.,<sup>75</sup> retweeted or responded to tweets posted to these IRA-controlled accounts. Multiple individuals affiliated with the Trump Campaign also promoted IRA tweets (discussed below).

### b. IRA Botnet Activities [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>69</sup>69

<sup>70</sup>70

<sup>71</sup>71

<sup>72</sup>72

<sup>73</sup>73

<sup>74</sup>74

<sup>75</sup>75

<sup>76</sup>76

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

[illegible][illegible]

In January 2018, Twitter publicly identified 3,814 Twitter accounts associated with the IRA.<sup>79</sup> 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."<sup>80</sup> 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.<sup>81</sup>

## 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 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.<sup>82</sup> The IRA

7777

7878

7979

8080

8181

8282

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

then further promoted the event by contacting U.S. media about the event and directing them to speak with the coordinator.<sup>83</sup> After the event, the IRA posted videos and photographs of the event to the IRA's social media accounts.<sup>84</sup>

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.<sup>85</sup> 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] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[illegible]

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

---

8383

8484

8585



## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

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).<sup>86</sup>

[illegible]

## 6. Targeting and Recruitment of U.S. Persons

[illegible][illegible]

IRA employees frequently used [REDACTED] [REDACTED] [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] [REDACTED] [REDACTED] [REDACTED] and a number of black social justice activists while posing as a grassroots group called "Black Matters US."<sup>89</sup> 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 Fist. The IRA

8686

8787

8888

8989

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

also recruited moderators of conservative social media groups to promote IRA-generated content,<sup>90</sup> 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).<sup>91</sup>

[illegible]

██████ ██████████ ██████████ 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). ██████████ ██████████ ██████████ ██████████

[illegible][illegible]

9090

9191

9292

9393

9494

9595

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

\_\_\_\_\_

## 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.,<sup>96</sup> Eric Trump,<sup>97</sup> Kellyanne Conway,<sup>98</sup> Brad Parscale,<sup>99</sup> and Michael T. Flynn.<sup>100</sup> These posts included allegations of voter fraud,<sup>101</sup> as well as allegations that Secretary Clinton had mishandled classified information.<sup>102</sup>
- A November 7, 2016 post from the IRA-controlled Twitter account Pamela\_Moore13 was retweeted by Donald J. Trump Jr.<sup>103</sup>

9696

9797

9898

9999

 $^{100}_{100}$ 

101 101

 $^{102}_{102}$ 

103103

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

- On September 19, 2017, President Trump’s personal account realDonaldTrump responded to a tweet from the IRA-controlled account 10\_gop (the backup account of TEN\_GOP, which had already been deactivated by Twitter). The tweet read: “We love you, Mr. President!”<sup>104</sup>

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!”<sup>105</sup> 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]

**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,<sup>107</sup> as well as requests to promote the rallies and help coordinate logistics.<sup>108</sup> 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.

---

<sup>104</sup>104

<sup>105</sup>105

<sup>106</sup>106

<sup>107</sup>107

<sup>108</sup>108

## II. RUSSIAN “ACTIVE MEASURES” SOCIAL MEDIA CAMPAIGN

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 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.

Open Source Draft

### III. Russian Hacking and Dumping Operations

[illegible]

### A. GRU Hacking Directed at the Clinton Campaign

## 1. GRU Units Target the Clinton Campaign

109 109



### III. RUSSIAN HACKING AND DUMPING OPERATIONS

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.<sup>117</sup>

The GRU spearphishing operation enabled it to gain access to numerous email accounts of Clinton Campaign employees and volunteers, including campaign chairman John Podesta, junior volunteers assigned to the Clinton Campaign's advance team, informal Clinton Campaign advisors, and a DNC employee.<sup>118</sup> 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.<sup>119</sup>

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<sup>120</sup> between the DCCC and DNC networks.<sup>121</sup> 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.<sup>122</sup>

#### **b. Implantation of Malware on DCCC and DNC Networks**

Unit 26165 implanted on the DCCC and DNC networks two types of customized malware,<sup>123</sup> known as "X-Agent" and "X-Tunnel"; Mimikatz,

---

<sup>117</sup><sup>117</sup>

<sup>118</sup><sup>118</sup>

<sup>119</sup><sup>119</sup>

<sup>120</sup><sup>120</sup>

<sup>121</sup><sup>121</sup>

<sup>122</sup><sup>122</sup>

<sup>123</sup><sup>123</sup>



### III. RUSSIAN HACKING AND DUMPING OPERATIONS

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).<sup>124</sup> 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.<sup>125</sup> GRU officers then used X-Tunnel 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.<sup>126</sup> 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] [REDACTED] served as a nerve center through which GRU officers monitored and directed the malware's operations on the DNC/DCCC networks.<sup>127</sup>

[illegible]

124124

125125

126126

127 127

128128

129 129

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

[REDACTED]

[REDACTED]

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.<sup>130</sup>

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."<sup>131</sup> 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.<sup>132</sup> The GRU appears

---

<sup>130</sup>130

<sup>131</sup>131

<sup>132</sup>132

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

to have compressed and exfiltrated over 70 gigabytes of data from this file server.<sup>133</sup>

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.<sup>134</sup> 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.<sup>135</sup> During these connections, Unit 26165 officers appear to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016.<sup>136</sup>

#### 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.<sup>137</sup> Unit 26165 paid for the registration using a pool of bitcoin that it had mined.<sup>138</sup> 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.

---

<sup>133</sup>133

<sup>134</sup>134

<sup>135</sup>135

<sup>136</sup>136

<sup>137</sup>137

<sup>138</sup>138

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

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.<sup>139</sup> 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.<sup>140</sup>

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

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.<sup>143</sup> 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.<sup>144</sup>

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

---

<sup>139</sup>139

<sup>140</sup>140

<sup>141</sup>141

<sup>142</sup>142

<sup>143</sup>143

<sup>144</sup>144

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

#### 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.<sup>145</sup> 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.<sup>146</sup>

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.<sup>147</sup> Released documents included opposition research performed by the DNC (including a memorandum analyzing 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."<sup>148</sup> The GRU later sent the reporter a password and link to a locked portion of the dcleaks.com website that

---

<sup>145</sup>145

<sup>146</sup>146

<sup>147</sup>147

<sup>148</sup>148

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

contained an archive of emails stolen by Unit 26165 from a Clinton Campaign volunteer in March 2016.<sup>149</sup> 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.<sup>150</sup>

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.<sup>151</sup> 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.<sup>152</sup> 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.<sup>153</sup>

[illegible]

149149

150150

151 151

152152

153153

154154

155155

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

#### 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 would [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, sadistic sociopath."<sup>156</sup>

In March 2016, WikiLeaks released a searchable archive of approximately 30,000 Clinton emails that had been obtained through FOIA litigation.<sup>157</sup> 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 US election, because eit [sic] may encourage people to send us even more important leaks.<sup>158</sup>

##### 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.

---

<sup>156</sup>156

<sup>157</sup>157

<sup>158</sup>158

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

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."<sup>159</sup> [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [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."<sup>160</sup>

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 twoo [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."<sup>161</sup>

**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 to WikiLeaks, [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [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] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]. [REDACTED]

---

<sup>159</sup>159

<sup>160</sup>160

<sup>161</sup>161



### III. RUSSIAN HACKING AND DUMPING OPERATIONS

[illegible]

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."<sup>163</sup> The email contained an encrypted attachment with the name "wk dnc link1.txt.gpg."<sup>164</sup> Using the Guccifer 2.0 Twitter account, GRU officers sent WikiLeaks an encrypted file and instructions on how to open it.<sup>165</sup> 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."<sup>166</sup> On July 22, 2016, WikiLeaks released over 20,000 emails and other documents stolen from the DNC computer networks.<sup>167</sup> 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."<sup>168</sup> 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.<sup>169</sup> 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 emails.<sup>170</sup>

An analysis of the metadata collected from the WikiLeaks site revealed that the stolen Podesta emails show a creation date of September 19, 2016.<sup>171</sup> 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

 $^{162}_{162}$ 

163163

164164

165 165

166166

167 167

168168

169169

170170

171 171

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

transfer to WikiLeaks (as the GRU had previously done in July 2016 for the DNC emails).<sup>172</sup> 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.<sup>173</sup>

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."<sup>174</sup> [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]  
[REDACTED]

[REDACTED].

[illegible]

On October 7, 2016, WikiLeaks released the first emails stolen from the 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;<sup>177</sup> internal communications between Podesta and other high-ranking members of the Clinton Campaign;<sup>178</sup> and

172172

173173

174174

175175

176 176

177177

178

110

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

correspondence related to the Clinton Foundation.<sup>179</sup> 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."<sup>180</sup> 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."<sup>181</sup>

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

---

<sup>179</sup>179

<sup>180</sup>180

<sup>181</sup>181

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

the DNC hack was an "inside job," and purported to have "physical proof" that Russians did not give materials to Assange.<sup>182</sup>

#### 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] [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."<sup>183</sup> 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] [REDACTED] including an email account belonging to Clinton aide [REDACTED] [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.<sup>184</sup>

Unit 26165 officers also hacked into a DNC account hosted on a cloud-computing service [REDACTED] [REDACTED]. On September 20, 2016, the GRU began to generate copies of the DNC data [REDACTED] [REDACTED] function designed to allow users to produce backups of databases (referred to [REDACTED] [REDACTED] as "snapshots"). The GRU then stole those snapshots by moving them to [REDACTED] [REDACTED] account that they controlled; from there, the copies were moved to GRU-controlled computers. The GRU stole approximately 300

---

<sup>182</sup>182

<sup>183</sup>183

<sup>184</sup>184

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

gigabytes of data from the DNC cloud-based account.<sup>185</sup>

#### 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.<sup>186</sup> 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.<sup>187</sup> 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).<sup>188</sup> 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,<sup>189</sup> and extracted data related to thousands of U.S. voters before the malicious activity was identified.<sup>190</sup>

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

---

<sup>185</sup>185

<sup>186</sup>186

<sup>187</sup>187

<sup>188</sup>188

<sup>189</sup>189

<sup>190</sup>190

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] for vulnerabilities on websites of more than two dozen states. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]. Similar [REDACTED] [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.<sup>191</sup> 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.<sup>192</sup> 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

[illegible]

1. [Harm to Ongoing Matter]

### a. Background

---

191 191

192









### III. RUSSIAN HACKING AND DUMPING OPERATIONS

[REDACTED] 217  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]. According to Malloch, Corsi asked him to put Corsi in touch with Assange, whom Corsi wished to interview. Malloch recalled that Corsi also suggested that individuals in the "orbit" of U.K. politician Nigel Farage might be able to contact Assange and asked if Malloch knew them. Malloch told Corsi that he would think about the request but made no actual attempt to connect Corsi with Assange.<sup>218</sup>

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] 219  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] 220

Malloch stated to investigators that beginning in or about August 2016, he and Corsi had multiple FaceTime discussions about WikiLeaks [REDACTED] [REDACTED] [REDACTED] had made a connection to Assange and that the hacked emails of John Podesta would be released prior to Election Day and would be helpful to the Trump Campaign. In one conversation in or around August or September 2016, Corsi told Malloch that the release of the Podesta emails was coming, after which "we" were going to be in the driver's seat.<sup>221</sup>

[REDACTED]  
[REDACTED] 222  
[REDACTED]  
[REDACTED] 223

---

<sup>217</sup>217

<sup>218</sup>218

<sup>219</sup>219

<sup>220</sup>220

<sup>221</sup>221

<sup>222</sup>222

<sup>223</sup>223

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

[illegible]

$^{224}_{224}$   
 $^{225}_{225}$   
 $^{226}_{226}$   
 $^{227}_{227}$   
 $^{228}_{228}$   
 $^{229}_{229}$   
 $^{230}_{230}$   
 $^{231}_{231}$   
 $^{232}_{232}$   
 $^{233}_{233}$   
 $^{234}_{234}$   
 $^{235}_{235}$

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] 236 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] 237 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] 238 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

#### d. WikiLeaks's October 7, 2016 Release of Stolen Podesta Emails

On October 7, 2016, four days after the Assange press conference [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED], the Washington Post published an Access Hollywood video that captured comments by candidate Trump some years earlier and that was expected to adversely affect the Campaign.<sup>239</sup> Less than an hour after the video's publication, WikiLeaks released the first set of emails stolen by the GRU from the account of Clinton Campaign chairman John Podesta.

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] 240 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] 241 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] 242 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] 243 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]. Corsi said that, because he had no direct means of communicating with WikiLeaks, he told members of the news site WND - who were participating on a conference call with him that

---

<sup>236</sup>236

<sup>237</sup>237

<sup>238</sup>238

<sup>239</sup>239

<sup>240</sup>240

<sup>241</sup>241

<sup>242</sup>242

<sup>243</sup>243

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

day - to reach Assange immediately.<sup>244</sup> Corsi claimed that the pressure was enormous and recalled telling the conference call the Access Hollywood tape was coming.<sup>245</sup> Corsi stated that he was convinced that his efforts had caused WikiLeaks to release the emails when they did.<sup>246</sup> In a later November 2018 interview, Corsi stated that he thought that he had told people on a WND conference call about the forthcoming tape and had sent out a tweet asking whether anyone could contact Assange, but then said that maybe he had done nothing.<sup>247</sup>

The Office investigated Corsi's allegations about the events of October 7, 2016 but found little corroboration for his allegations about the day.<sup>248</sup>

[REDACTED]

[REDACTED] 249

250

However, the phone records themselves do not indicate that the conversation was with any of the reporters who broke the Access Hollywood story, and the Office has not otherwise been able to identify the substance of the conversation. [REDACTED]

[REDACTED] [REDACTED].<sup>251</sup> However, the Office has not identified any conference call participant, or anyone who spoke to Corsi that day, who says that they received non-public information about the tape from Corsi or acknowledged having contacted a member of WikiLeaks on October 7, 2016 after a conversation with Corsi.

**e. Donald Trump Jr. Interaction with WikiLeaks** Donald Trump Jr. had direct electronic communications with WikiLeaks during the campaign period. On September 20, 2016, an individual named Jason Fishbein sent WikiLeaks the password for an unlaunched website focused on

---

244244

245245

246246

247247

248248

249 249

250250

251 251

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

Trump's "unprecedented and dangerous" ties to Russia, PutinTrump.org.<sup>252</sup> WikiLeaks publicly tweeted: "'Let's bomb Iraq' Progress for America PAC to launch 'PutinTrump.org' at 9:30am. Oops pw is 'putintrump' putintrump.org." Several hours later, WikiLeaks sent a Twitter direct message to Donald Trump Jr., "A PAC run anti-Trump site putintrump.org is about to launch. The PAC is a recycled pro-Iraq war PAC. We have guessed the password. It is 'putintrump.' See 'About' for who is behind it. Any comments ?"<sup>253</sup>

Several hours later, Trump Jr. emailed a variety of senior campaign staff:

Guys I got a weird Twitter DM from wikileaks. See below. I tried the password and it works and the about section they reference contains the next pic in terms of who is behind it. Not sure if this is anything but it seems like it's really wikileaks asking me as I follow them and it is a DM. Do you know the people mentioned and what the conspiracy they are looking for could be? These are just screen shots but it's a fully built out page claiming to be a PAC let me know your thoughts and if we want to look into it.<sup>254</sup>

Trump Jr. attached a screenshot of the "About" page for the unlaunched site PutinTrump.org. The next day (after the website had launched publicly), Trump Jr. sent a direct message to WikiLeaks: "Off the record, I don't know who that is but I'll ask around. Thanks."<sup>255</sup>

On October 3, 2016, WikiLeaks sent another direct message to Trump Jr., asking "you guys" to help disseminate a link alleging candidate Clinton had advocated using a drone to target Julian Assange. Trump Jr. responded that he already "had done so," and asked, "what's behind this Wednesday leak I keep reading about?"<sup>256</sup> WikiLeaks did not respond.

On October 12, 2016, WikiLeaks wrote again that it was "great to see you and your dad talking about our publications. Strongly suggest your dad tweets this link if he mentions us wlsearch.tk."<sup>257</sup> WikiLeaks wrote that the

---

<sup>252</sup>252

<sup>253</sup>253

<sup>254</sup>254

<sup>255</sup>255

<sup>256</sup>256

<sup>257</sup>257

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

link would help Trump in "digging through" leaked emails and stated, "we just released Podesta emails Part 4."<sup>258</sup> Two days later, Trump Jr. publicly tweeted the wlsearch.tk link.<sup>259</sup>

#### 2. Other Potential Campaign Interest in Russian Hacked Materials

Throughout 2016, the Trump Campaign expressed interest in Hillary Clinton's private email server and whether approximately 30,000 emails from that server had in fact been permanently destroyed, as reported by the media. Several individuals associated with the Campaign were contacted in 2016 about various efforts to obtain the missing Clinton emails and other stolen material in support of the Trump Campaign. Some of these contacts were met with skepticism, and nothing came of them; others were pursued to some degree. The investigation did not find evidence that the Trump Campaign recovered any such Clinton emails, or that these contacts were part of a coordinated effort between Russia and the Trump Campaign.

**a. Henry Oknyansky (a/k/a Henry Greenberg)** In the spring of 2016, Trump Campaign advisor Michael Caputo learned through a Florida-based Russian business partner that another Florida-based Russian, Henry Oknyansky (who also went by the name Henry Greenberg), claimed to have information pertaining to Hillary Clinton. Caputo notified Roger Stone and brokered communication between Stone and Oknyansky. Oknyansky and Stone set up a May 2016 in-person meeting.<sup>260</sup>

Oknyansky was accompanied to the meeting by Alexei Rasin, a Ukrainian associate involved in Florida real estate. At the meeting, Rasin offered to sell Stone derogatory information on Clinton that Rasin claimed to have obtained while working for Clinton. Rasin claimed to possess financial statements demonstrating Clinton's involvement in money laundering with Rasin's companies. According to Oknyansky, Stone asked if the amounts in question totaled millions of dollars but was told it was closer to hundreds of thousands. Stone refused the offer, stating that Trump would not pay for opposition research.<sup>261</sup>

---

<sup>258</sup>258

<sup>259</sup>259

<sup>260</sup>260

<sup>261</sup>261

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

Oknyansky claimed to the Office that Rasin's motivation was financial. According to Oknyansky, Rasin had tried unsuccessfully to shop the Clinton information around to other interested parties, and Oknyansky would receive a cut if the information was sold.<sup>262</sup> Rasin is noted in public source documents as the director and/or registered agent for a number of Florida companies, none of which appears to be connected to Clinton. The Office found no other evidence that Rasin worked for Clinton or any Clinton-related entities.

In their statements to investigators, Oknyansky and Caputo had contradictory recollections about the meeting. Oknyansky claimed that Caputo accompanied Stone to the meeting and provided an introduction, whereas Caputo did not tell us that he had attended and claimed that he was never told what information Oknyansky offered. Caputo also stated that he was unaware Oknyansky sought to be paid for the information until Stone informed him after the fact.<sup>263</sup>

The Office did not locate Rasin in the United States, although the Office confirmed Rasin had been issued a Florida driver's license. The Office otherwise was unable to determine the content and origin of the information he purportedly offered to Stone. Finally, the investigation did not identify evidence of a connection between the outreach or the meeting and Russian interference efforts.

**b. Campaign Efforts to Obtain Deleted Clinton Emails** After candidate Trump stated on July 27, 2016, that he hoped Russia would "find the 30,000 emails that are missing," Trump asked individuals affiliated with his Campaign to find the deleted Clinton emails.<sup>264</sup> Michael Flynn - who would later serve as National Security Advisor in the Trump Administration - recalled that Trump made this request repeatedly, and Flynn subsequently contacted multiple people in an effort to obtain the emails.<sup>265</sup>

Barbara Ledeen and Peter Smith were among the people contacted by Flynn. Ledeen, a long-time Senate staffer who had previously sought the Clinton emails, provided updates to Flynn about her efforts throughout the summer of 2016.<sup>266</sup> Smith, an investment advisor who was active in

---

<sup>262</sup>262

<sup>263</sup>263

<sup>264</sup>264

<sup>265</sup>265

<sup>266</sup>266



### III. RUSSIAN HACKING AND DUMPING OPERATIONS

Republican politics, also attempted to locate and obtain the deleted Clinton emails.<sup>267</sup>

Ledeen began her efforts to obtain the Clinton emails before Flynn's request, as early as December 2015.<sup>268</sup> On December 3, 2015, she emailed Smith a proposal to obtain the emails, stating, "Here is the proposal I briefly mentioned to you. The person I described to you would be happy to talk with you either in person or over the phone. The person can get the emails which 1. Were classified and 2. Were purloined by our enemies. That would demonstrate what needs to be demonstrated."<sup>269</sup>

Attached to the email was a 25-page proposal stating that the "Clinton email server was, in all likelihood, breached long ago," and that the Chinese, Russian, and Iranian intelligence services could "re-assemble the server's email content."<sup>270</sup> The proposal called for a three-phase approach. The first two phases consisted of open-source analysis. The third phase consisted of checking with certain intelligence sources "that have access through liaison work with various foreign services" to determine if any of those services had gotten to the server. The proposal noted, "Even if a single email was recovered and the providence [sic] of that email was a foreign service, it would be catastrophic to the Clinton campaign[.]" Smith forwarded the email to two colleagues and wrote, "we can discuss to whom it should be referred."<sup>271</sup> On December 16, 2015, Smith informed Ledeen that he declined to participate in her "initiative." According to one of Smith's business associates, Smith believed Ledeen's initiative was not viable at that time.<sup>272</sup>

Just weeks after Trump's July 2016 request to find the Clinton emails, however, Smith tried to locate and obtain the emails himself. He created a company, raised tens of thousands of dollars, and recruited security experts and business associates. Smith made claims to others involved in the effort (and those from whom he sought funding) that he was in contact with hackers with "ties and affiliations to Russia" who had access to the emails, and that his efforts were coordinated with the Trump Campaign.<sup>273</sup>

On August 28, 2016, Smith sent an email from an encrypted account with

---

<sup>267</sup><sup>267</sup>

<sup>268</sup><sup>268</sup>

<sup>269</sup><sup>269</sup>

<sup>270</sup><sup>270</sup>

<sup>271</sup><sup>271</sup>

<sup>272</sup><sup>272</sup>

<sup>273</sup><sup>273</sup>

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

the subject "Sec. Clinton's unsecured private email server" to an undisclosed list of recipients, including Campaign co-chairman Sam Clovis. The email stated that Smith was "[j]ust finishing two days of sensitive meetings here in DC with involved groups to poke and probe on the above. It is clear that the Clinton's home-based, unprotected server was hacked with ease by both State-related players, and private mercenaries. Parties with varying interests, are circling to release ahead of the election."<sup>274</sup>

On September 2, 2016, Smith directed a business associate to establish KLS Research LLC in furtherance of his search for the deleted Clinton emails.<sup>275</sup> One of the purposes of KLS Research was to manage the funds Smith raised in support of his initiative.<sup>276</sup> KLS Research received over \$30,000 during the presidential campaign, although Smith represented that he raised even more money.<sup>277</sup>

Smith recruited multiple people for his initiative, including security experts to search for and authenticate the emails.<sup>278</sup> In early September 2016, as part of his recruitment and fundraising effort, Smith circulated a document stating that his initiative was "in coordination" with the Trump Campaign, "to the extent permitted as an independent expenditure organization."<sup>279</sup> The document listed multiple individuals affiliated with the Trump Campaign, including Flynn, Clovis, Bannon, and Kellyanne Conway.<sup>280</sup> The investigation established that Smith communicated with at least Flynn and Clovis about his search for the deleted Clinton emails,<sup>281</sup> but the Office did not identify evidence that any of the listed individuals initiated or directed Smith's efforts.

In September 2016, Smith and Ledeen got back in touch with each other about their respective efforts. Ledeen wrote to Smith, "wondering if you had some more detailed reports or memos or other data you could share because we have come a long way in our efforts since we last visited.... We would need as much technical discussion as possible so we could marry it against the new data we have found and then could share it back to you 'your eyes

---

<sup>274</sup>274

<sup>275</sup>275

<sup>276</sup>276

<sup>277</sup>277

<sup>278</sup>278

<sup>279</sup>279

<sup>280</sup>280

<sup>281</sup>281

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

only.’”<sup>282</sup>

Ledeen claimed to have obtained a trove of emails (from what she described as the “dark web”) that purported to be the deleted Clinton emails. Ledeen wanted to authenticate the emails and solicited contributions to fund that effort. Erik Prince provided funding to hire a tech advisor to ascertain the authenticity of the emails. According to Prince, the tech advisor determined that the emails were not authentic.<sup>283</sup>

A backup of Smith’s computer contained two files that had been downloaded from WikiLeaks and that were originally attached to emails received by John Podesta. The files on Smith’s computer had creation dates of October 2, 2016, which was prior to the date of their release by WikiLeaks. Forensic examination, however, established that the creation date did not reflect when the files were downloaded to Smith’s computer. (It appears the creation date was when WikiLeaks staged the document for release, as discussed in Volume I, Section III.B.3.c, *supra*.<sup>284</sup>) The investigation did not otherwise identify evidence that Smith obtained the files before their release by WikiLeaks.

Smith continued to send emails to an undisclosed recipient list about Clinton’s deleted emails until shortly before the election. For example, on October 28, 2016, Smith wrote that there was a “tug-of-war going on within WikiLeaks over its planned releases in the next few days,” and that WikiLeaks “has maintained that it will save its best revelations for last, under the theory this allows little time for response prior to the U.S. election November 8.”<sup>285</sup> An attachment to the email claimed that WikiLeaks would release “All 33k deleted Emails” by “November 1st.” No emails obtained from Clinton’s server were subsequently released.

Smith drafted multiple emails stating or intimating that he was in contact with Russian hackers. For example, in one such email, Smith claimed that, in August 2016, KLS Research had organized meetings with parties who had access to the deleted Clinton emails, including parties with “ties and affiliations to Russia.”<sup>286</sup> The investigation did not identify evidence that any such meetings occurred. Associates and security experts who worked with Smith on the initiative did not believe that Smith was in contact with

---

<sup>282</sup>282

<sup>283</sup>283

<sup>284</sup>284

<sup>285</sup>285

<sup>286</sup>286

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

Russian hackers and were aware of no such connection.<sup>287</sup> The investigation did not establish that Smith was in contact with Russian hackers or that Smith, Ledeen, or other individuals in touch with the Trump Campaign ultimately obtained the deleted Clinton emails.

In sum, the investigation established that the GRU hacked into email accounts of persons affiliated with the Clinton Campaign, as well as the computers of the DNC and DCCC. The GRU then exfiltrated data related to the 2016 election from these accounts and computers, and disseminated that data through fictitious online personas (DCLeaks and Guccifer 2.0) and later through WikiLeaks. The investigation also established that the Trump Campaign displayed interest in the WikiLeaks releases, and that [REDACTED] [REDACTED]. As explained in Volume I, Section V.B, infra, the evidence was sufficient to support computer-intrusion (and other) charges against GRU officers for their role in election-related hacking. [REDACTED] [REDACTED].

287287

IV. RUSSIAN GOVERNMENT LINKS TO AND CONTACTS WITH  
THE TRUMP CAMPAIGN

**IV. Russian Government Links to and Con-  
tacts with The Trump Campaign**

**A. Campaign Period (September 2015 - November 8,  
2016)**

**1. Trump Tower Moscow Project**

**a. Trump Tower Moscow Venture with the Crocus Group (2013-  
2014)**

**b. Communications with I.C. Expert Investment Company and  
Giorgi Rtskhiladze (Summer and Fall 2015)**

**c. Letter of Intent and Contacts to Russian Government (October  
2015-January 2016)**

**i. Trump Signs the Letter of Intent on behalf of the Trump  
Organization**

**ii. Post-LOI Contacts with Individuals in Russia**

**d. Discussions about Russia Travel by Michael Cohen or Candi-  
date Trump (December 2015-June 2016)**

**i. Sater's Overtures to Cohen to Travel to Russia**

**ii. Candidate Trump's Opportunities to Travel to Russia**

**2. George Papadopoulos**

**a. Origins of Campaign Work**

**b. Initial Russia-Related Contacts**

**c. March 31 Foreign Policy Team Meeting**

#### IV. RUSSIAN GOVERNMENT LINKS TO AND CONTACTS WITH THE TRUMP CAMPAIGN

d. George Papadopoulos Learns That Russia Has "Dirt" in the  
Form of Clinton Emails

e. Russia-Related Communications With The Campaign

f. Trump Campaign Knowledge of "Dirt"

g. Additional George Papadopoulos Contact

3. Carter Page

a. Background

b. Origins of and Early Campaign Work

c. Carter Page's July 2016 Trip To Moscow

d. Later Campaign Work and Removal from the Campaign

4. Dimitri Simes and the Center for the National Interest

a. CNI and Dimitri Simes Connect with the Trump Campaign

b. National Interest Hosts a Foreign Policy Speech at the  
Mayflower Hotel

c. Jeff Sessions's Post-Speech Interactions with CNI

d. Jared Kushner's Continuing Contacts with Simes

5. June 9, 2016 Meeting at Trump Tower

a. Setting Up the June 9 Meeting

i. Outreach to Donald Trump Jr

ii. Awareness of the Meeting Within the Campaign

#### IV. RUSSIAN GOVERNMENT LINKS TO AND CONTACTS WITH THE TRUMP CAMPAIGN

##### b. The Events of June 9, 2016

- i. Arrangements for the Meeting
- ii. Conduct of the Meeting

##### c. Post-June 9 Events

#### 6. Events at the Republican National Convention

##### a. Ambassador Kislyak's Encounters with Senator Sessions and J.D. Gordon the Week of the RNC

##### b. Change to Republican Party Platform

#### 7. Post-Convention Contacts with Kislyak

##### a. Ambassador Kislyak Invites J.D. Gordon to Breakfast at the Ambassador's Residence

##### b. Senator Sessions's September 2016 Meeting with Ambassador Kislyak

#### 8. Paul Manafort

##### a. Paul Manafort's Ties to Russia and Ukraine

- i. Oleg Deripaska Consulting Work
- ii. Political Consulting Work
- iii. Konstantin Kilimnik

##### b. Contacts during Paul Manafort's Time with the Trump Cam- paign

- i. Paul Manafort Joins the Campaign

#### **IV. RUSSIAN GOVERNMENT LINKS TO AND CONTACTS WITH THE TRUMP CAMPAIGN**

##### **ii. Paul Manafort's Campaign-Period Contacts**

##### **iii. Paul Manafort's Two Campaign-Period Meetings with Konstantin Kilimnik in the United States**

##### **c. Post-Resignation Activities**

#### **B. Post-Election and Transition-Period Contacts**

##### **1. Immediate Post-Election Activity**

##### **a. Outreach from the Russian Government**

##### **b. High-Level Encouragement of Contacts through Alternative Channels**

##### **2. Kirill Dmitriev's Transition-Era Outreach to the Incoming Ad- ministration**

##### **a. Background**

##### **b. Kirill Dmitriev's Post-Election Contacts With the Incoming Administration**

##### **c. Erik Prince and Kirill Dmitriev Meet in the Seychelles**

##### **i. George Nader and Erik Prince Arrange Seychelles Meeting with Dmitriev**

##### **ii. The Seychelles Meetings**

##### **iii. Erik Prince's Meeting with Steve Bannon after the Sey- chelles Trip**

##### **d. Kirill Dmitriev's Post-Election Contact with Rick Gerson Re- garding U.S.-Russia Relations**



#### IV. RUSSIAN GOVERNMENT LINKS TO AND CONTACTS WITH THE TRUMP CAMPAIGN

3. Ambassador Kislyak's Meeting with Jared Kushner and Michael Flynn in Trump Tower Following the Election
4. Jared Kushner's Meeting with Sergey Gorkov
5. Petr Aven's Outreach Efforts to the Transition Team
6. Carter Page Contact with Deputy Prime Minister Arkady Dvorkovich
7. Contacts With and Through Michael T. Flynn
  - a. United Nations Vote on Israeli Settlements
  - b. U.S. Sanctions Against Russia

Open Source Draft

## V. PROSECUTION AND DECLINATION DECISIONS

### V. Prosecution and Declination Decisions

#### A. Russian "Active Measures" Social Media Campaign

#### B. Russian Hacking and Dumping Operations

##### 1. Section 1030 Computer-Intrusion Conspiracy

###### a. Background

###### b. Charging Decision As to [ ] : Harm to Ongoing Matter]

##### 2. Potential Section 1030 Violation By [ ] : Personal Privacy]

#### C. Russian Government Outreach and Contacts

##### 1. Potential Coordination: Conspiracy and Collusion

##### 2. Potential Coordination: Foreign Agent Statutes (FARA and 18 U.S.C. § 951)

###### a. Governing Law

###### b. Application

##### 3. Campaign Finance

###### a. Overview Of Governing Law

###### b. Application to June 9 Trump Tower Meeting

###### i. Thing-of-Value Element

###### ii. Willfulness

###### iii. Difficulties in Valuing Promised Information

###### c. Application to WikiLeaks [ ] : HOM]

## V. PROSECUTION AND DECLINATION DECISIONS

- i. Questions Over [ : Harm to Ongoing Matter]
  - ii. Willfulness
  - iii. Constitutional Considerations
  - iv. Analysis [ : HOM]
4. False Statements and Obstruction of the Investigation
- a. Overview Of Governing Law
  - b. Application to Certain Individuals
    - i. George Papadopoulos
    - ii. [ : Personal Privacy]
    - iii. Michael Flynn
    - iv. Michael Cohen
    - v. [ : HOM]
    - vi. Jeff Sessions
    - vii. Others Interviewed During the Investigation