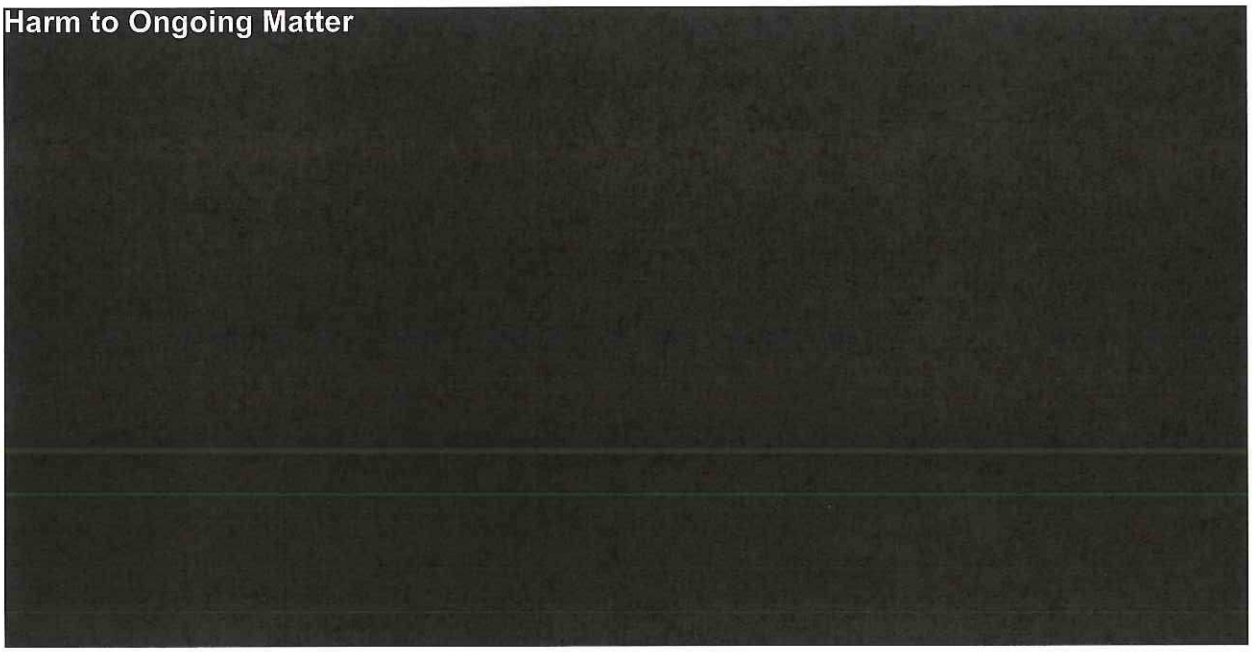


7. Interactions and Contacts with the Trump Campaign

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

a. Trump Campaign Promotion of IRA Political Materials

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

- Posts from the IRA-controlled Twitter account @TEN_GOP were cited or retweeted by multiple Trump Campaign officials and surrogates, including Donald J. Trump Jr.,[96] Eric

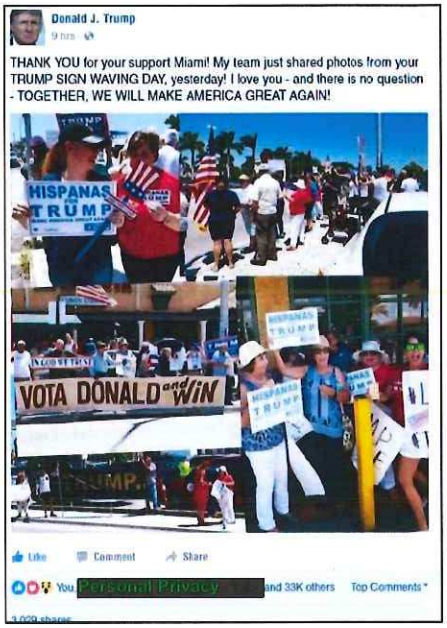
[96] *See, e.g.*, @DonaldJTrumpJr 10/26/16 Tweet ("RT @TEN_GOP: BREAKING Thousands of names changed on voter rolls in Indiana. Police investigating #VoterFraud. #DrainTheSwamp."); @DonaldJTrumpJr 11/2/16 Tweet ("RT @TEN_GOP: BREAKING: #VoterFraud by counting tens of thousands of ineligible mail in Hillary votes being reported in Broward County, Florida."); @DonaldJTrumpJr 11/8/16 Tweet ("RT @TEN_GOP: This vet passed away last month before he could vote for Trump. Here he is in his #MAGA hat. #voted #ElectionDay."). Trump Jr. retweeted additional @TEN_GOP content subsequent to the election.

Trump,[97] Kellyanne Conway,[98] Brad Parscale,[99] and Michael T. Flynn.[100] These posts included allegations of voter fraud,[101] as well as allegations that Secretary Clinton had mishandled classified information.[102]

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

- On September 19, 2017, President Trump's personal account @realDonaldTrump responded to a tweet from the IRA-controlled account @10_gop (the backup account of @TEN_GOP, which had already been deactivated by Twitter). The tweet read: "We love you, Mr. President!"[104]

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



Screenshot of Trump Facebook Account (from Matt Skiber)

---

[97] @EricTrump 10/20/16 Tweet ("RT @TEN_GOP: BREAKING Hillary shuts down press conference when asked about DNC Operatives corruption & #VoterFraud #debatenight #TrumpB").

[98] @KellyannePolls 11/6/16 Tweet ("RT @TEN_GOP: Mother of jailed sailor: 'Hold Hillary to same standards as my son on Classified info' #hillarysemail #WeinerGate.").

[99] @parscale 10/15/16 Tweet ("Thousands of deplorables chanting to the media: 'Tell The Truth!' RT if you are also done w/ biased Media! #FridayFeeling").

[100] @GenFlynn 11/7/16 (retweeting @TEN_GOP post that included in part "@realDonaldTrump & @mike_pence will be our next POTUS & VPOTUS.").

[101] @TEN_GOP 10/11/16 Tweet ("North Carolina finds 2,214 voters over the age of 110!!").

[102] @TEN_GOP 11/6/16 Tweet ("Mother of jailed sailor: 'Hold Hillary to same standards as my son on classified info #hillaryemail #WeinerGate.'").

[103] @DonaldJTrumpJr 11/7/16 Tweet ("RT @Pamela_Moore13: Detroit residents speak out against the failed policies of Obama, Hillary & democrats . . . .").

[104] @realDonaldTrump 9/19/17 (7:33 p.m.) Tweet ("THANK YOU for your support Miami! My team just shared photos from your TRUMP SIGN WAVING DAY, yesterday! I love you – and there is no question – TOGETHER, WE WILL MAKE AMERICA GREAT AGAIN!").

[105] 8/23/16 Facebook Message, ID 100009922908461 (Matt Skiber) to ID PP [redacted]

Harm to Ongoing Matter [106]

b. Contact with Trump Campaign Officials in Connection to Rallies

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

* * *

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

---

[106] Harm to Ongoing Matter

[107] *See, e.g.*, 8/16/16 Email, joshmilton024@gmail.com to PP @donaldtrump.com (asking for Trump/Pence signs for Florida rally); 8/18/16 Email, joshmilton024@gmail.com to PP @donaldtrump.com (asking for Trump/Pence signs for Florida rally); 8/12/16 Email, joshmilton024@gmail.com to PP @donaldtrump.com (asking for "contact phone numbers for Trump Campaign affiliates" in various Florida cities and signs).

[108] 8/15/16 Email, Personal Privacy to joshmilton024@gmail.com (asking to add to locations to the "Florida Goes Trump," list); 8/16/16 Email, Personal Privacy to joshmilton024@gmail.com (volunteering to send an email blast to followers).

III. Russian Hacking and Dumping Operations

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

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

A. GRU Hacking Directed at the Clinton Campaign

1. GRU Units Target the Clinton Campaign

Two military units of the GRU carried out the computer intrusions into the Clinton Campaign, DNC, and DCCC: Military Units 26165 and 74455.[110] Military Unit 26165 is a GRU cyber unit dedicated to targeting military, political, governmental, and non-governmental organizations outside of Russia, including in the United States.[111] The unit was sub-divided into departments with different specialties. One department, for example, developed specialized malicious software ("malware"), while another department conducted large-scale spearphishing campaigns.[112] Investigative Technique [redacted] a bitcoin mining operation to

---

[109] As discussed in Section V below, our Office charged 12 GRU officers for crimes arising from the hacking of these computers, principally with conspiring to commit computer intrusions, in violation of 18 U.S.C. §§1030 and 371. *See* Volume I, Section V.B, *infra*; Indictment, *United States v. Netyksho*, No. 1:18-cr-215 (D.D.C. July 13, 2018), Doc. 1 ("*Netyksho* Indictment").

[110] *Netyksho* Indictment ¶ 1.

[111] Separate from this Office's indictment of GRU officers, in October 2018 a grand jury sitting in the Western District of Pennsylvania returned an indictment charging certain members of Unit 26165 with hacking the U.S. Anti-Doping Agency, the World Anti-Doping Agency, and other international sport associations. *United States v. Aleksei Sergeyevich Morenets*, No. 18-263 (W.D. Pa.).

[112] A spearphishing email is designed to appear as though it originates from a trusted source, and solicits information to enable the sender to gain access to an account or network, or causes the recipient to

secure bitcoins used to purchase computer infrastructure used in hacking operations.[113]

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

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

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

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

The GRU spearphishing operation enabled it to gain access to numerous email accounts of Clinton Campaign employees and volunteers, including campaign chairman John Podesta, junior volunteers assigned to the Clinton Campaign's advance team, informal Clinton Campaign advisors, and a DNC employee.[118] GRU officers stole tens of thousands of emails from spearphishing victims, including various Clinton Campaign-related communications.

---

download malware that enables the sender to gain access to an account or network. *Netyksho* Indictment ¶ 10.

[113] Bitcoin mining consists of unlocking new bitcoins by solving computational problems. IT [redacted] kept its newly mined coins in an account on the bitcoin exchange platform CEX.io. To make purchases, the GRU routed funds into other accounts through transactions designed to obscure the source of funds. *Netyksho* Indictment ¶ 62.

[114] *Netyksho* Indictment ¶ 69.

[115] *Netyksho* Indictment ¶ 9.

[116] *See* SM-2589105, serials 144 & 495.

[117] Investigative Technique [redacted]

[118] Investigative Technique [redacted]

2. Intrusions into the DCCC and DNC Networks

a. Initial Access

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

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

b. Implantation of Malware on DCCC and DNC Networks

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

---

[119] Investigative Technique

[120] A VPN extends a private network, allowing users to send and receive data across public networks (such as the internet) as if the connecting computer was directly connected to the private network. The VPN in this case had been created to give a small number of DCCC employees access to certain databases housed on the DNC network. Therefore, while the DCCC employees were outside the DNC's private network, they could access parts of the DNC network from their DCCC computers.

[121] Investigative Technique
SM-2589105-HACK, serial 5.

[122] Investigative Technique
M-2589105-HACK, serial 5.

[123] "Malware" is short for malicious software, and here refers to software designed to allow a third party to infiltrate a computer without the consent or knowledge of the computer's user or operator.

[124] Investigative Technique

[125] Investigative Technique

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

The AMS Panel used to control X-Agent during the DCCC and DNC intrusions was housed on a leased computer located near IT Arizona.[128] Investigative Technique [129]

Investigative Technique

Investigative Technique

[126] In connection with these intrusions, the GRU used computers (virtual private networks, dedicated servers operated by hosting companies, etc.) that it leased from third-party providers located all over the world. The investigation identified rental agreements and payments for computers located in, *inter alia*, Investigative Technique all of which were used in the operations targeting the U.S. election.

[127] *Netyksho* Indictment ¶ 25.

[128] *Netyksho* Indictment ¶ 24(c).

[129] *Netyksho* Indictment ¶ 24(b).

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 keylogging sessions included passwords, internal communications between employees, banking information, and sensitive personal information.

c. Theft of Documents from DNC and DCCC Networks

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

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

The GRU also stole documents from the DNC network shortly after gaining access. On April 22, 2016, the GRU copied files from the DNC network to GRU-controlled computers. Stolen documents included the DNC's opposition research into candidate Trump.[134] Between approximately May 25, 2016 and June 1, 2016, GRU officers accessed the DNC's mail server from a GRU-controlled computer leased inside the United States.[135] During these connections,

---

[130] *Netyksho* Indictment ¶¶ 27-29; Investigative Technique

[131] Investigative Technique

[132] Investigative Technique

[133] Investigative Technique

[134] Investigative Technique

SM-2589105-HACK, serial 5. Investigative Technique

[135] Investigative Technique

See SM-2589105-GJ, serial 649. As part of its investigation, the FBI later received images of DNC servers and copies of relevant traffic logs. *Netyksho* Indictment ¶¶ 28-29.

Unit 26165 officers appear to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016.[136]

B. Dissemination of the Hacked Materials

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

1. DCLeaks

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

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

---

[136] *Netyksho* Indictment ¶ 29. The last-in-time DNC email released by WikiLeaks was dated May 25, 2016, the same period of time during which the GRU gained access to the DNC's email server. *Netyksho* Indictment ¶ 45.

[137] *Netyksho* Indictment ¶ 35. Approximately a week before the registration of dcleaks.com, the same actors attempted to register the website electionleaks.com using the same domain registration service. Investigative Technique

[138] *See* SM-2589105, serial 181; *Netyksho* Indictment ¶ 21(a).

[139] Investigative Technique

[140] *See, e.g.*, Internet Archive, "https://dcleaks.com/" (archive date Nov. 10, 2016). Additionally, DCLeaks released documents relating to Personal Privacy, emails belonging to PP, and emails from 2015 relating to Republican Party employees (under the portfolio name "The United States Republican Party"). "The United States Republican Party" portfolio contained approximately 300 emails from a variety of GOP members, PACs, campaigns, state parties, and businesses dated between May and October 2015. According to open-source reporting, these victims shared the same

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

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

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

2. Guccifer 2.0

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

Tennessee-based web-hosting company, called Smartech Corporation. William Bastone, *RNC E-Mail Was, In Fact, Hacked By Russians*, The Smoking Gun (Dec. 13, 2016).

[141] *Netyksho* Indictment ¶ 38.

[142] *See, e.g.*, Facebook Account 100008825623541 (Alice Donovan).

[143] 7/14/16 Facebook Message, ID 793058100795341 (DC Leaks) to ID Personal Privacy

[144] *See, e.g.*, 9/14/16 Twitter DM, @dcleaks_ to Personal Privacy; 9/14/16 Twitter DM, @dcleaks_ to Personal Privacy. The messages read: "Hi https://t.co/QTvKUjQcOx pass: KvFsg%*14@gPgu& enjoy ;)."

[145] Dmitri Alperovitch, *Bears in the Midst: Intrusion into the Democratic National Committee*, CrowdStrike Blog (June 14, 2016). CrowdStrike updated its post after the June 15, 2016 post by Guccifer 2.0 claiming responsibility for the intrusion.

[146] *Netyksho* Indictment ¶¶ 41-42.

That same day, June 15, 2016, the GRU also used the Guccifer 2.0 WordPress blog to begin releasing to the public documents stolen from the DNC and DCCC computer networks. The Guccifer 2.0 persona ultimately released thousands of documents stolen from the DNC and DCCC in a series of blog posts between June 15, 2016 and October 18, 2016.[147] Released documents included opposition research performed by the DNC (including a memorandum analyzing potential criticisms of candidate Trump), internal policy documents (such as recommendations on how to address politically sensitive issues), analyses of specific congressional races, and fundraising documents. Releases were organized around thematic issues, such as specific states (*e.g.*, Florida and Pennsylvania) that were perceived as competitive in the 2016 U.S. presidential election.

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

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

---

[147] Releases of documents on the Guccifer 2.0 blog occurred on June 15, 2016; June 20, 2016; June 21, 2016; July 6, 2016; July 14, 2016; August 12, 2016; August 15, 2016; August 21, 2016; August 31, 2016; September 15, 2016; September 23, 2016; October 4, 2016; and October 18, 2016.

[148] 6/27/16 Email, guccifer20@aol.fr to Personal Privacy (subject "leaked emails"); IT .

[149] 6/27/16 Email, guccifer20@aol.fr to Personal Privacy (subject "leaked emails"); IT ; *see also* 6/27/16 Email, guccifer20@aol.fr to Personal Privacy (subject "leaked emails"); IT (claiming DCLeaks was a "Wikileaks sub project").

[150] Before sending the reporter the link and password to the closed DCLeaks website, and in an apparent effort to deflect attention from the fact that DCLeaks and Guccifer 2.0 were operated by the same organization, the Guccifer 2.0 persona sent the reporter an email stating that DCLeaks was a "Wikileaks sub project" and that Guccifer 2.0 had asked DCLeaks to release the leaked emails with "closed access" to give reporters a preview of them.

[151] *Netyksho* Indictment ¶ 43(a).

[152] *Netyksho* Indictment ¶ 43(b).

[153] *Netyksho* Indictment ¶ 43(c).

The GRU was also in contact through the Guccifer 2.0 persona with HOM a former Trump Campaign member Harm to Ongoing Matter [154] In early August 2016, HOM Twitter's suspension of the Guccifer 2.0 Twitter account. After it was reinstated, GRU officers posing as Guccifer 2.0 wrote HOM via private message, "thank u for writing back . . . do u find anyt[h]ing interesting in the docs i posted?" On August 17, 2016, the GRU added, "please tell me if i can help u anyhow . . . it would be a great pleasure to me." On September 9, 2016, the GRU—again posing as Guccifer 2.0—referred to a stolen DCCC document posted online and asked HOM "what do u think of the info on the turnout model for the democrats entire presidential campaign." HOM responded, "pretty standard."[155] The investigation did not identify evidence of other communications between HOM and Guccifer 2.0.

3. Use of WikiLeaks

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

a. WikiLeaks's Expressed Opposition Toward the Clinton Campaign

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

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

---

[154] HOM

[155] Harm to Ongoing Matter

[156] 11/19/15 Twitter Group Chat, Group ID 594242937858486276, @WikiLeaks et al. Assange also wrote that, "GOP will generate a lot oposition [sic], including through dumb moves. Hillary will do the same thing, but co-opt the liberal opposition and the GOP opposition. Hence hillary has greater freedom to start wars than the GOP and has the will to do so." *Id.*

[157] WikiLeaks, "Hillary Clinton Email Archive," *available at* https://wikileaks.org/clinton-emails/.

> [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 en[]courage people to send us even more important leaks.[158]

b. WikiLeaks's First Contact with Guccifer 2.0 and DCLeaks

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

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

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

c. The GRU's Transfer of Stolen Materials to WikiLeaks

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

---

[158] 3/14/16 Twitter DM, @WikiLeaks to PP Less than two weeks earlier, the same account had been used to send a private message opposing the idea of Clinton "in whitehouse with her bloodlutt and amitions [sic] of empire with hawkish liberal-interventionist appointees." 11/19/15 Twitter Group Chat, Group ID 594242937858486276, @WikiLeaks et al.

[159] 6/14/16 Twitter DM, @dcleaks_ to @WikiLeaks.

[160] *Netyksho* Indictment ¶ 47(a).

[161] 7/6/16 Twitter DMs, @WikiLeaks & @guccifer_2.

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. Investigative Technique [redacted][62]

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

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

The same day, the Twitter account @guccifer_2 sent @dcleaks_ a direct message, which is the first known contact between the personas.[169] During subsequent communications, the

---

[162] Investigative Technique [redacted]

[163] This was not the GRU's first attempt at transferring data to WikiLeaks. On June 29, 2016, the GRU used a Guccifer 2.0 email account to send a large encrypted file to a WikiLeaks email account. 6/29/16 Email, guccifer2@mail.com IT [redacted] (The email appears to have been undelivered.)

[164] *See* SM-2589105-DCLEAKS, serial 28 (analysis).

[165] 6/27/16 Twitter DM, @Guccifer_2 to @WikiLeaks.

[166] 7/18/16 Twitter DM, @Guccifer_2 & @WikiLeaks.

[167] "DNC Email Archive," WikiLeaks (Jul. 22, 2016), *available at* https://wikileaks.org/dnc-emails.

[168] 9/15/16 Twitter DM, @dcleaks_ to @WikiLeaks.

[169] 9/15/16 Twitter DM, @guccifer_2 to @dcleaks_.

Guccifer 2.0 persona informed DCLeaks that WikiLeaks was trying to contact DCLeaks and arrange for a way to speak through encrypted emails.[170]

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

Beginning on September 20, 2016, WikiLeaks and DCLeaks resumed communications in a brief exchange. On September 22, 2016, a DCLeaks email account dcleaksproject@gmail.com sent an email to a WikiLeaks account with the subject "Submission" and the message "Hi from DCLeaks." The email contained a PGP-encrypted message with the filename "wiki_mail.txt.gpg."[174] Investigative Technique 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 Investigative Technique

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

---

[170] *See* SM-2589105-DCLEAKS, serial 28; 9/15/16 Twitter DM, @Guccifer_2 & @WikiLeaks.

[171] *See* SM-2284941, serials 63 & 64 Investigative Technique

[172] Investigative Technique At the time, certain Apple operating systems used a setting that left a downloaded file's creation date the same as the creation date shown on the host computer. This would explain why the creation date on WikiLeaks's version of the files was still September 19, 2016. *See* SM-2284941, serial 62 Investigative Technique

[173] When WikiLeaks saved attachments separately from the stolen emails, its computer system appears to have treated each attachment as a new file and given it a new creation date. *See* SM-2284941, serials 63 & 64.

[174] *See* 9/22/16 Email, dcleaksproject@gmail.com IT

[175] Ellen Nakashima et al., *A German Hacker Offers a Rare Look Inside the Secretive World of Julian Assange and WikiLeaks*, Washington Post (Jan. 17, 2018).

Investigative Technique [redacted] [176]

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

d. WikiLeaks Statements Dissembling About the Source of Stolen Materials

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

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

[176] Investigative Technique [redacted]

[177] Personal Privacy [redacted]

[178] Personal Privacy [redacted]

[179] *Netyksho* Indictment ¶ 43.

[180] @WikiLeaks 8/9/16 Tweet.

circumstances, it doesn't necessarily mean that the two are connected. But it is a very serious matter…that type of allegation is very serious, as it's taken very seriously by us."[181]

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

C. 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.

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

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

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

---

[181] *See Assange: "Murdered DNC Staffer Was 'Potential' WikiLeaks Source,"* Fox News (Aug. 25, 2016)(containing video of Assange interview by Megyn Kelly).

[182] M. Raju & Z. Cohen, *A GOP Congressman's Lonely Quest Defending Julian Assange*, CNN (May 23, 2018).

[183] "Donald Trump on Russian & Missing Hillary Clinton Emails," YouTube Channel C-SPAN, Posted 7/27/16, *available at* https://www.youtube.com/watch?v=3kxG8uJUsWU (starting at 0:41).

[184] Investigative Technique [redacted]

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

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

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

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

GRU officers Investigative Technique scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers [redacted] Investigative Technique for vulnerabilities on websites of more than two dozen states. Investigative Technique

[185] *Netyksho* Indictment ¶ 34; *see also* SM-2589105-HACK, serial 29 Investigative Technique [redacted].

[186] *Netyksho* Indictment ¶ 69.

[187] *Netyksho* Indictment ¶ 69; Investigative Technique [redacted]

[188] Investigative Technique [redacted]

[189] Investigative Technique [redacted]

[190] Investigative Technique [redacted]

Investigative Technique

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

D. Trump Campaign and the Dissemination of Hacked Materials

The Trump Campaign showed interest in WikiLeaks's releases of hacked materials throughout the summer and fall of 2016. Harm to Ongoing Matter

1. HOM

a. Background

Harm to Ongoing Matter

[191] *Netyksho* Indictment ¶ 76; Investigative Technique

[192] Investigative Technique

b. Contacts with the Campaign about WikiLeaks

Harm to Ongoing Matter [93]

Harm to Ongoing Matter

On June 12, 2016, Assange claimed in a televised interview to "have emails relating to Hillary Clinton which are pending publication,"[194] but provided no additional context.

In debriefings with the Office, former deputy campaign chairman Rick Gates said that, Harm to Ongoing Matter [195]

Harm to Ongoing Matter

Gates recalled candidate Trump being generally frustrated that the Clinton emails had not been found.[196]

Paul Manafort, who would later become campaign chairman, Harm to Ongoing Matter [197] Harm to Ongoing Matter [198]

---

[193] Harm to Ongoing Matter

[194] *See* Mahita Gajanan, *Julian Assange Timed DNC Email Release for Democratic Convention*, Time (July 27, 2016) (quoting the June 12, 2016 television interview).

[195] In February 2018, Gates pleaded guilty, pursuant to a plea agreement, to a superseding criminal information charging him with conspiring to defraud and commit multiple offenses (*i.e.*, tax fraud, failure to report foreign bank accounts, and acting as an unregistered agent of a foreign principal) against the United States, as well as making false statements to our Office. Superseding Criminal Information, *United States v. Richard W. Gates III*, 1:17-cr-201 (D.D.C. Feb. 23, 2018), Doc. 195 ("*Gates* Superseding Criminal Information"); Plea Agreement, *United States v. Richard W. Gates III*, 1:17-cr-201 (D.D.C. Feb. 23, 2018), Doc. 205 ("*Gates* Plea Agreement"). Gates has provided information and in-court testimony that the Office has deemed to be reliable.

[196] Gates 10/25/18 302, at 1-2.

[197] As explained further in Volume I, Section IV.A.8, *infra*, Manafort entered into a plea agreement with our Office. We determined that he breached the agreement by being untruthful in proffer sessions and before the grand jury. We have generally recounted his version of events in this report only when his statements are sufficiently corroborated to be trustworthy; to identify issues on which Manafort's untruthful responses may themselves be of evidentiary value; or to provide Manafort's explanations for certain events, even when we were unable to determine whether that explanation was credible. His account appears here principally because it aligns with those of other witnesses.

[198] Grand Jury

Michael Cohen, former executive vice president of the Trump Organization and special counsel to Donald J. Trump,[199] told the Office that he recalled an incident in which he was in candidate Trump's office in Trump Tower Harm to Ongoing Matter [200] Harm to Ongoing Matter [201] Cohen further told the Office that, after WikiLeaks's subsequent release of stolen DNC emails in July 2016, candidate Trump said to Cohen something to the effect of, HOM [202]

Harm to Ongoing Matter According to Gates, Manafort expressed excitement about the release HOM [203] Manafort, for his part, told the Office that, shortly after WikiLeaks's July 22 release, Manafort also spoke with candidate Trump Harm to Ongoing Matter [204] Harm to Ongoing Matter [205] Manafort also HOM wanted to be kept apprised of any

[199] In November 2018, Cohen pleaded guilty pursuant to a plea agreement to a single-count information charging him with making false statements to Congress, in violation of 18 U.S.C. § 1001(a) & (c). He had previously pleaded guilty to several other criminal charges brought by the U.S. Attorney's Office in the Southern District of New York, after a referral from this Office. In the months leading up to his false-statements guilty plea, Cohen met with our Office on multiple occasions for interviews and provided information that the Office has generally assessed to be reliable and that is included in this report.

[200] HOM

[201] Harm to Ongoing Matter

[202] Cohen 9/18/18 302, at 10. Harm to Ongoing Matter Harm to Ongoing Matter Harm to Ongoing Matter

[203] Gates 10/25/18 302 (serial 241), at 4.

[204] Grand Jury

[205] Grand Jury

developments with WikiLeaks and separately told Gates to keep in touch HOM about future WikiLeaks releases.[206]

According to Gates, by the late summer of 2016, the Trump Campaign was planning a press strategy, a communications campaign, and messaging based on the possible release of Clinton emails by WikiLeaks.[207] Harm to Ongoing Matter [208] Harm to Ongoing Matter while Trump and Gates were driving to LaGuardia Airport. Harm to Ongoing Matter, shortly after the call candidate Trump told Gates that more releases of damaging information would be coming.[209]

Harm to Ongoing Matter [10]

c. Harm to Ongoing Matter

Harm to Ongoing Matter [11]

Corsi is an author who holds a doctorate in political science.[212] In 2016, Corsi also worked for the media outlet WorldNetDaily (WND). Harm to Ongoing Matter [13]

---

[206] Grand Jury

[207] Gates 4/10/18 302, at 3; Gates 4/11/18 302, at 1-2 (SM-2180998); Gates 10/25/18 302, at 2.

[208] HOM

[209] Gates 10/25/18 302 (serial 241), at 4.

[210] HOM

[211] HOM

[212] Corsi first rose to public prominence in August 2004 when he published his book *Unfit for Command: Swift Boat Veterans Speak Out Against John Kerry*. In the 2008 election cycle, Corsi gained prominence for being a leading proponent of the allegation that Barack Obama was not born in the United States. Corsi told the Office that Donald Trump expressed interest in his writings, and that he spoke with Trump on the phone on at least six occasions. Corsi 9/6/18 302, at 3.

[213] Corsi 10/31/18 302, at 2; Grand Jury Corsi was first interviewed on September 6, 2018 at the Special Counsel's offices in Washington, D.C. He was accompanied by counsel throughout the interview. Corsi was subsequently interviewed on September 17, 2018; September 21, 2018; October 31, 2018; November 1, 2018; and November 2, 2018. Counsel was

Harm to Ongoing Matter [14] Corsi told the Office during interviews that he "must have" previously discussed Assange with Malloch.[215] Harm to Ongoing Matter [216] Harm to Ongoing Matter [217]

Grand Jury 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.[218]

Harm to Ongoing Matter [19] Harm to Ongoing Matter [20]

present for all interviews, and the interviews beginning on September 21, 2018 were conducted pursuant to a proffer agreement that precluded affirmative use of his statements against him in limited circumstances.

[214] HOM

[215] Corsi 10/31/18 302, at 4.

[216] HOM

[217] HOM

[218] Grand Jury Malloch denied ever communicating with Assange or WikiLeaks, stating that he did not pursue the request to contact Assange because he believed he had no connections to Assange. Grand Jury

[219] HOM

[220] Harm to Ongoing Matter

Malloch stated to investigators that beginning in or about August 2016, he and Corsi had multiple FaceTime discussions about WikiLeaks Harm to Ongoing Matter 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.[221]

Harm to Ongoing Matter

[222] Harm to Ongoing Matter

[23] Harm to Ongoing Matter

[24] Harm to Ongoing Matter

[225]

Harm to Ongoing Matter

[226] Harm to Ongoing Matter

[27] Harm to Ongoing Matter

[228])

Harm to Ongoing Matter

[229] Harm to Ongoing Matter

---

[221] Grand Jury

[222] Harm to Ongoing Matter

[223] Harm to Ongoing Matter

[224] Harm to Ongoing Matter

[225] Harm to Ongoing Matter

[226] Harm to Ongoing Matter

[227] Harm to Ongoing Matter

[228] HOM

[229] Harm to Ongoing Matter

Harm to Ongoing Matter 230
Harm to Ongoing Matter

231 Harm to Ongoing Matter

232

Harm to Ongoing Matter

33 Harm to Ongoing Matter

234 Harm to Ongoing Matter

235

Harm to Ongoing Matter

236 Harm to Ongoing Matter

237

Harm to Ongoing Matter

238

Harm to Ongoing Matter

230 Harm to Ongoing Matter

231 Harm to Ongoing Matter

232 HOM

233 Harm to Ongoing Matter

234 Harm to Ongoing Matter

235 Harm to Ongoing Matter

236 Harm to Ongoing Matter

237 HOM

238 Harm to Ongoing Matter

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

On October 7, 2016, four days after the Assange press conference HOM , 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.[239] 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.

Harm to Ongoing Matter

[240] Harm to Ongoing Matter

[241] Harm to Ongoing Matter

[242]

Harm to Ongoing Matter

[43] Harm to Ongoing Matter

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 day—to reach Assange immediately.[244] Corsi claimed that the pressure was

---

Harm to Ongoing Matter

[239] Candidate Trump can be heard off camera making graphic statements about women.

[240] HOM

[241] HOM

[242] HOM

[243] HOM

[244] In a later November 2018 interview, Corsi stated Harm to Ongoing Matter that he believed Malloch was on the call but then focused on other individuals who were on the call-invitation, which Malloch was not. (Separate travel records show that at the time of the call, Malloch was aboard a transatlantic flight). Corsi at one point stated that after WikiLeaks's release of stolen emails on October 7, 2016, he concluded Malloch had gotten in contact with Assange. Corsi 11/1/18 302, at 6.

enormous and recalled telling the conference call the *Access Hollywood* tape was coming.[245] Corsi stated that he was convinced that his efforts had caused WikiLeaks to release the emails when they did.[246] 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.[247]

The Office investigated Corsi's allegations about the events of October 7, 2016 but found little corroboration for his allegations about the day.[248] Harm to Ongoing Matter [249] Harm to Ongoing Matter [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. Harm to Ongoing Matter [251] 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 Trump's "unprecedented and dangerous" ties

---

[245] During the same interview, Corsi also suggested that he may have sent out public tweets because he knew Assange was reading his tweets. Our Office was unable to find evidence of any such tweets.

[246] Corsi 9/21/18 302, at 6-7.

[247] Corsi 11/1/18 302, at 6.

[248] Harm to Ongoing Matter Grand Jury

[249] Harm to Ongoing Matter

[250] HOM Grand Jury Harm to Ongoing Matter

[251] HOM Grand Jury Harm to Ongoing Matter Grand Jury Harm to Ongoing Matter

to Russia, PutinTrump.org.[252] 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?"[253]

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.[254]

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."[255]

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?"[256] 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."[257] WikiLeaks wrote that the link would help Trump in "digging through" leaked emails and stated, "we just released Podesta emails Part 4."[258] Two days later, Trump Jr. publicly tweeted the wlsearch.tk link.[259]

---

[252] 9/20/16 Twitter DM, @JasonFishbein to @WikiLeaks; *see* JF00587 (9/21/16 Messages, PP @jabber.cryptoparty.is & PP @jabber.cryptoparty.is); Fishbein 9/5/18 302, at 4. When interviewed by our Office, Fishbein produced what he claimed to be logs from a chatroom in which the participants discussed U.S. politics; one of the other participants had posted the website and password that Fishbein sent to WikiLeaks.

[253] 9/20/16 Twitter DM, @WikiLeaks to @DonaldJTrumpJr.

[254] TRUMPORG_28_000629-33 (9/21/16 Email, Trump Jr. to Conway et al. (subject "Wikileaks")).

[255] 9/21/16 Twitter DM, @DonaldJTrumpJr to @WikiLeaks.

[256] 10/3/16 Twitter DMs, @DonaldJTrumpJr & @WikiLeaks.

[257] At the time, the link took users to a WikiLeaks archive of stolen Clinton Campaign documents.

[258] 10/12/16 Twitter DM, @WikiLeaks to @DonaldJTrumpJr.

[259] @DonaldJTrumpJr 10/14/16 (6:34 a.m.) Tweet.

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.[260]

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.[261]

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.[262] 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.[263]

---

[260] Caputo 5/2/18 302, at 4; Oknyansky 7/13/18 302, at 1.

[261] Oknyansky 7/13/18 302, at 1-2.

[262] Oknyansky 7/13/18 302, at 2.

[263] Caputo 5/2/18 302, at 4; Oknyansky 7/13/18 302, at 1.

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.[264] 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.[265]

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.[266] Smith, an investment advisor who was active in Republican politics, also attempted to locate and obtain the deleted Clinton emails.[267]

Ledeen began her efforts to obtain the Clinton emails before Flynn's request, as early as December 2015.[268] 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."[269]

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."[270] 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

---

[264] Flynn 4/25/18 302, at 5-6; Flynn 5/1/18 302, at 1-3.

[265] Flynn 5/1/18 302, at 1-3.

[266] Flynn 4/25/18 302, at 7; Flynn 5/4/18 302, at 1-2; Flynn 11/29/17 302, at 7-8.

[267] Flynn 11/29/17 302, at 7.

[268] Szobocsan 3/29/17 302, at 1.

[269] 12/3/15 Email, Ledeen to Smith.

[270] 12/3/15 Email, Ledeen to Smith (attachment).

wrote, "we can discuss to whom it should be referred."[271] 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.[272]

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.[273]

On August 28, 2016, Smith sent an email from an encrypted account with 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."[274]

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

Smith recruited multiple people for his initiative, including security experts to search for and authenticate the emails.[278] 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."[279] The document listed multiple individuals affiliated with the Trump Campaign, including Flynn, Clovis, Bannon,

---

[271] 12/3/15 Email, Smith to Szobocsan & Safron.

[272] Szobocsan 3/29/18 302, at 1.

[273] 8/31/16 Email, Smith to Smith.

[274] 8/28/16 Email, Smith to Smith.

[275] Incorporation papers of KLS Research LLC, 7/26/17 Grand Jury [redacted] Szobocsan 3/29/18 302, at 2.

[276] Szobocsan 3/29/18 302, at 3.

[277] Financial Institution Record of Peter Smith and KLS Research LLC, 10/31/17 [redacted] Grand Jury [redacted] 10/11/16 Email, Smith to Personal Privacy [redacted]

[278] Tait 8/22/17 302, at 3; York 7/12/17 302, at 1-2; York 11/22/17 302, at 1.

[279] York 7/13/17 302 (attachment KLS Research, LLC, "Clinton Email Reconnaissance Initiative," Sept. 9, 2016).

and Kellyanne Conway.[280] The investigation established that Smith communicated with at least Flynn and Clovis about his search for the deleted Clinton emails,[281] 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 only.'"[282]

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.[283]

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*.[284]) 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."[285] An attachment to the

---

[280] The same recruitment document listed Jerome Corsi under "Independent Groups/Organizations/Individuals," and described him as an "established author and writer from the right on President Obama and Sec. Clinton."

[281] Flynn 11/29/17 302, at 7-8; 10/15/16 Email, Smith to Flynn et al.; 8/28/16 Email, Smith to Smith (bcc: Clovis et al.).

[282] 9/16/16 Email, Ledeen to Smith.

[283] Prince 4/4/18 302, at 4-5.

[284] The forensic analysis of Smith's computer devices found that Smith used an older Apple operating system that would have preserved that October 2, 2016 creation date when it was downloaded (no matter what day it was in fact downloaded by Smith). *See* Volume I, Section III.B.3.c, *supra*. The Office tested this theory in March 2019 by downloading the two files found on Smith's computer from WikiLeaks's site using the same Apple operating system on Smith's computer; both files were successfully downloaded and retained the October 2, 2016 creation date. *See* SM-2284941, serial 62.

[285] 10/28/16 Email, Smith to Smith.

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."[286] 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 Russian hackers and were aware of no such connection.[287] 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 Harm to Ongoing Matter 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. Harm to Ongoing Matter

[286] 8/31/16 Email, Smith to Smith.

[287] Safron 3/20/18 302, at 3; Szobocsan 3/29/18 302, at 6.

IV. Russian Government Links To And Contacts With The Trump Campaign

The Office identified multiple contacts—"links," in the words of the Appointment Order—between Trump Campaign officials and individuals with ties to the Russian government. The Office investigated whether those contacts constituted a third avenue of attempted Russian interference with or influence on the 2016 presidential election. In particular, the investigation examined whether these contacts involved or resulted in coordination or a conspiracy with the Trump Campaign and Russia, including with respect to Russia providing assistance to the Campaign in exchange for any sort of favorable treatment in the future. Based on the available information, the investigation did not establish such coordination.

This Section describes the principal links between the Trump Campaign and individuals with ties to the Russian government, including some contacts with Campaign officials or associates that have been publicly reported to involve Russian contacts. Each subsection begins with an overview of the Russian contact at issue and then describes in detail the relevant facts, which are generally presented in chronological order, beginning with the early months of the Campaign and extending through the post-election, transition period.

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

Russian-government-connected individuals and media entities began showing interest in Trump's campaign in the months after he announced his candidacy in June 2015.[288] Because Trump's status as a public figure at the time was attributable in large part to his prior business and entertainment dealings, this Office investigated whether a business contact with Russia-linked individuals and entities during the campaign period—the Trump Tower Moscow project, *see* Volume I, Section IV.A.1, *infra*—led to or involved coordination of election assistance.

Outreach from individuals with ties to Russia continued in the spring and summer of 2016, when Trump was moving toward—and eventually becoming—the Republican nominee for President. As set forth below, the Office also evaluated a series of links during this period: outreach to two of Trump's then-recently named foreign policy advisors, including a representation that Russia had "dirt" on Clinton in the form of thousands of emails (Volume I, Sections IV.A.2 & IV.A.3); dealings with a D.C.-based think tank that specializes in Russia and has connections with its government (Volume I, Section IV.A.4); a meeting at Trump Tower between the Campaign and a Russian lawyer promising dirt on candidate Clinton that was "part of Russia and its government's support for [Trump]" (Volume I, Section IV.A.5); events at the Republican National Convention (Volume I, Section IV.A.6); post-Convention contacts between Trump Campaign officials and Russia's ambassador to the United States (Volume I, Section IV.A.7); and contacts through campaign chairman Paul Manafort, who had previously worked for a Russian oligarch and a pro-Russian political party in Ukraine (Volume I, Section IV.A.8).

---

[288] For example, on August 18, 2015, on behalf of the editor-in-chief of the internet newspaper *Vzglyad*, Georgi Asatryan emailed campaign press secretary Hope Hicks asking for a phone or in-person candidate interview. 8/18/15 Email, Asatryan to Hicks. One day earlier, the publication's founder (and former Russian parliamentarian) Konstantin Rykov had registered two Russian websites—Trump2016.ru and DonaldTrump2016.ru. No interview took place.

1. Trump Tower Moscow Project

The Trump Organization has pursued and completed projects outside the United States as part of its real estate portfolio. Some projects have involved the acquisition and ownership (through subsidiary corporate structures) of property. In other cases, the Trump Organization has executed licensing deals with real estate developers and management companies, often local to the country where the project was located.[289]

Between at least 2013 and 2016, the Trump Organization explored a similar licensing deal in Russia involving the construction of a Trump-branded property in Moscow. The project, commonly referred to as a "Trump Tower Moscow" or "Trump Moscow" project, anticipated a combination of commercial, hotel, and residential properties all within the same building. Between 2013 and June 2016, several employees of the Trump Organization, including then-president of the organization Donald J. Trump, pursued a Moscow deal with several Russian counterparties. From the fall of 2015 until the middle of 2016, Michael Cohen spearheaded the Trump Organization's pursuit of a Trump Tower Moscow project, including by reporting on the project's status to candidate Trump and other executives in the Trump Organization.[290]

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

The Trump Organization and the Crocus Group, a Russian real estate conglomerate owned and controlled by Aras Agalarov, began discussing a Russia-based real estate project shortly after the conclusion of the 2013 Miss Universe pageant in Moscow.[291] Donald J. Trump Jr. served as the primary negotiator on behalf of the Trump Organization; Emin Agalarov (son of Aras Agalarov) and Irakli "Ike" Kaveladze represented the Crocus Group during negotiations,[292] with the occasional assistance of Robert Goldstone.[293]

In December 2013, Kaveladze and Trump Jr. negotiated and signed preliminary terms of

---

[289] *See, e.g.*, *Interview of: Donald J. Trump, Jr, Senate Judiciary Committee*, 115th Cong. 151-52 (Sept. 7, 2017) (discussing licensing deals of specific projects).

[290] As noted in Volume I, Section III.D.1, *supra*, in November 2018, Cohen pleaded guilty to making false statements to Congress concerning, among other things, the duration of the Trump Tower Moscow project. *See* Information ¶ 7(a), *United States v. Michael Cohen*, 1:18-cr-850 (S.D.N.Y. Nov. 29, 2018), Doc. 2 ("*Cohen* Information").

[291] *See Interview of: Donald J. Trump, Jr, Senate Judiciary Committee,* 115th Cong. 13 (Sept. 7, 2017) ("Following the pageant the Trump Organization and Mr. Agalarov's company, Crocus Group, began preliminarily discussion [sic] potential real estate projects in Moscow."). As has been widely reported, the Miss Universe pageant—which Trump co-owned at the time—was held at the Agalarov-owned Crocus City Hall in Moscow in November 2013. Both groups were involved in organizing the pageant, and Aras Agalarov's son Emin was a musical performer at the event, which Trump attended.

[292] Kaveladze 11/16/17 302, at 2, 4-6; Grand Jury [redacted] OSC-KAV_00385 (12/6/13 Email, Trump Jr. to Kaveladze & E. Agalarov).

[293] Grand Jury [redacted]

an agreement for the Trump Tower Moscow project.[294] On December 23, 2013, after discussions with Donald J. Trump, the Trump Organization agreed to accept an arrangement whereby the organization received a flat 3.5% commission on all sales, with no licensing fees or incentives.[295] The parties negotiated a letter of intent during January and February 2014.[296]

From January 2014 through November 2014, the Trump Organization and Crocus Group discussed development plans for the Moscow project. Some time before January 24, 2014, the Crocus Group sent the Trump Organization a proposal for a 800-unit, 194-meter building to be constructed at an Agalarov-owned site in Moscow called "Crocus City," which had also been the site of the Miss Universe pageant.[297] In February 2014, Ivanka Trump met with Emin Agalarov and toured the Crocus City site during a visit to Moscow.[298] From March 2014 through July 2014, the groups discussed "design standards" and other architectural elements.[299] For example, in July 2014, members of the Trump Organization sent Crocus Group counterparties questions about the "demographics of these prospective buyers" in the Crocus City area, the development of neighboring parcels in Crocus City, and concepts for redesigning portions of the building.[300] In August 2014, the Trump Organization requested specifications for a competing Marriott-branded tower being built in Crocus City.[301]

Beginning in September 2014, the Trump Organization stopped responding in a timely fashion to correspondence and proposals from the Crocus Group.[302] Communications between the two groups continued through November 2014 with decreasing frequency; what appears to be the last communication is dated November 24, 2014.[303] The project appears not to have developed past the planning stage, and no construction occurred.

---

[294] Grand Jury

[295] OSC-KAV_00452 (12/23/13 Email, Trump Jr. to Kaveladze & E. Agalarov).

[296] *See, e.g.*, OSC-KAV_01158 (Letter agreement signed by Trump Jr. & E. Agalarov); OSC-KAV_01147 (1/20/14 Email, Kaveladze to Trump Jr. et al.).

[297] *See, e.g.*, OSC-KAV_00972 (10/14/14 Email, McGee to Khoo et al.) (email from Crocus Group contractor about specifications); OSC-KAV_00540 (1/24/14 Email, McGee to Trump Jr. et al.).

[298] *See* OSC-KAV_00631 (2/5/14 Email, E. Agalarov to Ivanka Trump, Trump Jr. & Kaveladze); Goldstone Facebook post, 2/4/14 (8:01 a.m.) Investigative Technique

[299] *See, e.g.*, OSC-KAV_00791 (6/3/14 Email, Kaveladze to Trump Jr. et al.; OSC-KAV_00799 (6/10/14 Email, Trump Jr. to Kaveladze et al.); OSC-KAV_00817 (6/16/14 Email, Trump Jr. to Kaveladze et al.).

[300] OSC-KAV_00870 (7/17/14 Email, Khoo to McGee et al.).

[301] OSC-KAV_00855 (8/4/14 Email, Khoo to McGee et al.).

[302] OSC-KAV_00903 (9/29/14 Email, Tropea to McGee & Kaveladze (noting last response was on August 26, 2014)); OSC-KAV_00906 (9/29/14 Email, Kaveladze to Tropea & McGee (suggesting silence "proves my fear that those guys are bailing out of the project")); OSC-KAV_00972 (10/14/14 Email, McGee to Khoo et al.) (email from Crocus Group contractor about development specifications)).

[303] OSC-KAV_01140 (11/24/14 Email, Khoo to McGee et al.).

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

In the late summer of 2015, the Trump Organization received a new inquiry about pursuing a Trump Tower project in Moscow. In approximately September 2015, Felix Sater, a New York-based real estate advisor, contacted Michael Cohen, then-executive vice president of the Trump Organization and special counsel to Donald J. Trump.[304] Sater had previously worked with the Trump Organization and advised it on a number of domestic and international projects. Sater had explored the possibility of a Trump Tower project in Moscow while working with the Trump Organization and therefore knew of the organization's general interest in completing a deal there.[305] Sater had also served as an informal agent of the Trump Organization in Moscow previously and had accompanied Ivanka Trump and Donald Trump Jr. to Moscow in the mid-2000s.[306]

Sater contacted Cohen on behalf of I.C. Expert Investment Company (I.C. Expert), a Russian real-estate development corporation controlled by Andrei Vladimirovich Rozov.[307] Sater had known Rozov since approximately 2007 and, in 2014, had served as an agent on behalf of Rozov during Rozov's purchase of a building in New York City.[308] Sater later contacted Rozov and proposed that I.C. Expert pursue a Trump Tower Moscow project in which I.C. Expert would license the name and brand from the Trump Organization but construct the building on its own. Sater worked on the deal with Rozov and another employee of I.C. Expert.[309]

Cohen was the only Trump Organization representative to negotiate directly with I.C. Expert or its agents. In approximately September 2015, Cohen obtained approval to negotiate with I.C. Expert from candidate Trump, who was then president of the Trump Organization. Cohen provided updates directly to Trump about the project throughout 2015 and into 2016, assuring him the project was continuing.[310] Cohen also discussed the Trump Moscow project with Ivanka Trump as to design elements (such as possible architects to use for the project[311]) and Donald J. Trump Jr. (about his experience in Moscow and possible involvement in the project[312]) during the fall of 2015.

---

[304] Sater provided information to our Office in two 2017 interviews conducted under a proffer agreement. Grand Jury

[305] Grand Jury

[306] Sater 9/19/17 302, at 1-2, 5.

[307] Sater 9/19/17 302, at 3.

[308] Rozov 1/25/18 302, at 1.

[309] Rozov 1/25/18 302, at 1; *see also* 11/2/15 Email, Cohen to Rozov et al. (sending letter of intent).

[310] Cohen 9/12/18 302, at 1-2, 4-6.

[311] Cohen 9/12/18 302, at 5.

[312] Cohen 9/12/18 302, at 4-5.

Also during the fall of 2015, Cohen communicated about the Trump Moscow proposal with Giorgi Rtskhiladze, a business executive who previously had been involved in a development deal with the Trump Organization in Batumi, Georgia.[313] Cohen stated that he spoke to Rtskhiladze in part because Rtskhiladze had pursued business ventures in Moscow, including a licensing deal with the Agalarov-owned Crocus Group.[314] On September 22, 2015, Cohen forwarded a preliminary design study for the Trump Moscow project to Rtskhiladze, adding "I look forward to your reply about this spectacular project in Moscow." Rtskhiladze forwarded Cohen's email to an associate and wrote, "[i]f we could organize the meeting in New York at the highest level of the Russian Government and Mr. Trump this project would definitely receive the worldwide attention."[315]

On September 24, 2015, Rtskhiladze sent Cohen an attachment that he described as a proposed "[l]etter to the Mayor of Moscow from Trump org," explaining that "[w]e need to send this letter to the Mayor of Moscow (second guy in Russia) he is aware of the potential project and will pledge his support."[316] In a second email to Cohen sent the same day, Rtskhiladze provided a translation of the letter, which described the Trump Moscow project as a "symbol of stronger economic, business and cultural relationships between New York and Moscow and therefore United States and the Russian Federation."[317] On September 27, 2015, Rtskhiladze sent another email to Cohen, proposing that the Trump Organization partner on the Trump Moscow project with "Global Development Group LLC," which he described as being controlled by Michail Posikhin, a Russian architect, and Simon Nizharadze.[318] Cohen told the Office that he ultimately declined the proposal and instead continued to work with I.C. Expert, the company represented by Felix Sater.[319]

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

Between approximately October 13, 2015 and November 2, 2015, the Trump Organization (through its subsidiary Trump Acquisition, LLC) and I.C. Expert completed a letter of intent (LOI) for a Trump Moscow property. The LOI, signed by Trump for the Trump Organization and Rozov on behalf of I.C. Expert, was "intended to facilitate further discussions" in order to "attempt to

---

[313] Rtskhiladze was a U.S.-based executive of the Georgian company Silk Road Group. In approximately 2011, Silk Road Group and the Trump Organization entered into a licensing agreement to build a Trump-branded property in Batumi, Georgia. Rtskhiladze was also involved in discussions for a Trump-branded project in Astana, Kazakhstan. The Office twice interviewed Rtskhiladze, [redacted] Grand Jury [redacted]

[314] Cohen 9/12/18 302, at 12; *see also* Rtskhiladze 5/10/18 302, at 1.

[315] 9/22/15 Email, Rtskhiladze to Nizharadze.

[316] 9/24/15 Email, Rtskhiladze to Cohen.

[317] 9/24/15 Email, Rtskhiladze to Cohen.

[318] 9/27/15 Email, Rtskhiladze to Cohen.

[319] Cohen 9/12/18 302, at 12.

enter into a mutually acceptable agreement" related to the Trump-branded project in Moscow.[320] The LOI contemplated a development with residential, hotel, commercial, and office components, and called for "[a]pproximately 250 first class, luxury residential condominiums," as well as "[o]ne first class, luxury hotel consisting of approximately 15 floors and containing not fewer than 150 hotel rooms."[321] For the residential and commercial portions of the project, the Trump Organization would receive between 1% and 5% of all condominium sales,[322] plus 3% of all rental and other revenue.[323] For the project's hotel portion, the Trump Organization would receive a base fee of 3% of gross operating revenues for the first five years and 4% thereafter, plus a separate incentive fee of 20% of operating profit.[324] Under the LOI, the Trump Organization also would receive a $4 million "up-front fee" prior to groundbreaking.[325] Under these terms, the Trump Organization stood to earn substantial sums over the lifetime of the project, without assuming significant liabilities or financing commitments.[326]

On November 3, 2015, the day after the Trump Organization transmitted the LOI, Sater emailed Cohen suggesting that the Trump Moscow project could be used to increase candidate Trump's chances at being elected, writing:

> Buddy our boy can become President of the USA and we can engineer it. I will get all of Putins team to buy in on this, I will manage this process. . . . Michael, Putin gets on stage with Donald for a ribbon cutting for Trump Moscow, and Donald owns the republican nomination. And possibly beats Hillary and our boy is in. . . . We will manage this process better than anyone. You and I will get Donald and Vladimir on a stage together very shortly. That the game changer.[327]

Later that day, Sater followed up:

> Donald doesn't stare down, he negotiates and understands the economic issues and Putin only want to deal with a pragmatic leader, and a successful business man is a good candidate for someone who knows how to negotiate. "Business, politics, whatever it all is the same for someone who knows how to deal"

---

[320] 11/2/15 Email, Cohen to Rozov et al. (attachment) (hereinafter "LOI"); *see also* 10/13/15 Email, Sater to Cohen & Davis (attaching proposed letter of intent).

[321] LOI, p. 2.

[322] The LOI called for the Trump Organization to receive 5% of all gross sales up to $100 million; 4% of all gross sales from $100 million to $250 million; 3% of all gross sales from $250 million to $500 million; 2% of all gross sales from $500 million to $1 billion; and 1% of all gross sales over $1 billion. LOI, Schedule 2.

[323] LOI, Schedule 2.

[324] LOI, Schedule 1.

[325] LOI, Schedule 2.

[326] Cohen 9/12/18 302, at 3.

[327] 11/3/15 Email, Sater to Cohen (12:14 p.m.).

> I think I can get Putin to say that at the Trump Moscow press conference.
> If he says it we own this election. Americas most difficult adversary agreeing that Donald is a good guy to negotiate. . . .
> We can own this election.
> Michael my next steps are very sensitive with Putins very very close people, we can pull this off.
> Michael lets go. 2 boys from Brooklyn getting a USA president elected. This is good really good.[328]

According to Cohen, he did not consider the political import of the Trump Moscow project to the 2016 U.S. presidential election at the time. Cohen also did not recall candidate Trump or anyone affiliated with the Trump Campaign discussing the political implications of the Trump Moscow project with him. However, Cohen recalled conversations with Trump in which the candidate suggested that his campaign would be a significant "infomercial" for Trump-branded properties.[329]

ii. Post-LOI Contacts with Individuals in Russia

Given the size of the Trump Moscow project, Sater and Cohen believed the project required approval (whether express or implicit) from the Russian national government, including from the Presidential Administration of Russia.[330] Sater stated that he therefore began to contact the Presidential Administration through another Russian business contact.[331] In early negotiations with the Trump Organization, Sater had alluded to the need for government approval and his attempts to set up meetings with Russian officials. On October 12, 2015, for example, Sater wrote to Cohen that "all we need is Putin on board and we are golden," and that a "meeting with Putin and top deputy is tentatively set for the 14th [of October]."[332] Grand Jury this meeting was being coordinated by associates in Russia and that he had no direct interaction with the Russian government.[333]

Approximately a month later, after the LOI had been signed, Lana Erchova emailed Ivanka Trump on behalf of Erchova's then-husband Dmitry Klokov, to offer Klokov's assistance to the Trump Campaign.[334] Klokov was at that time Director of External Communications for PJSC Federal Grid Company of Unified Energy System, a large Russian electricity transmission

---

[328] 11/3/15 Email, Sater to Cohen (12:40 p.m.).

[329] Cohen 9/12/18 302, at 3-4; Cohen 8/7/18 302, at 15.

[330] Grand Jury Sater 12/15/17 302, at 2.

[331] Sater 12/15/17 302, at 3-4.

[332] 10/12/15 Email, Sater to Cohen (8:07 a.m.).

[333] Grand Jury

[334] Ivanka Trump received an email from a woman who identified herself as "Lana E. Alexander," which said in part, "If you ask anyone who knows Russian to google my husband Dmitry Klokov, you'll see who he is close to and that he has done Putin's political campaigns." 11/16/15 Email, Erchova to I. Trump.