

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**. After **HOM** Wikileaks's first Clinton-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 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** 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. I :18-cr-215 (D.D.C. July 13, 2018), Doc. 1 ("Netyksho Indictment").

¹¹⁰ *Netyksho Indictment*, r 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 **Investigative Technique** to learn about **Investigative Technique** different Democratic websites, including democrats.org, hillaryclinton.com, dnc.com, and dccc.org. **Investigative Technique** 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. Ill 1111 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

¹¹⁸ Investigative Technique

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) connection¹²⁰ 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 server¹²².

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 XTunnel 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.

Investigative Technique

¹²¹ **Investigative Technique**

¹²² **Investigative Technique**

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 in a leased computer located near **Investigative Technique** Arizona¹²⁸ **Investigative Technique**

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 ,r 25.

¹²⁸ Netyksho Indictment ,r 24(c).

¹²⁹ Netyksho Indictment ,r 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 key logging sessions included passwords, internal communications between employees, banking information, and sensitive personal information.

c. Theft of Documents from DNC and DCCC Networks

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

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

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

—

¹³⁰ *Netyksho* Indictment ,r 27-29; **Investigative Technique**

¹³¹ **Investigative Technique**

¹³² **Investigative Technique**

¹³³ **Investigative Technique**

¹³³ **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 ,i,i 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 ,i 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 ,i 45.

¹³⁷ *Netyksho* Indictment ,i 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 ,i 2l(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 **Personal Privacy**, 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 ,r 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, ; 9/14/16 Twitter OM, **Personal Privacy** @dcleaks_ to **Personal Privacy** . The messages read: "Hi https://t.co/QTvKUjQcOx pass: KvFsgo/o* 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 ,r,r 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, uccifer20@aol.fr to **Personal Privacy** see also 612 7 /16 (subject "leaked emails"); project"). (sub' project "leaked emails" **Investigative Technique**

¹⁴⁹ 6/27/16 Email, uccifer20@aol.fr to **Personal Privacy** see also 612 7 /16 (subject "leaked emails"); project"). (sub' project "leaked emails" **Investigative Technique**

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 repmler 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 ,r 43(a).

¹⁵² *Netyksho* Indictment ,r 43(b).

¹⁵³ *Netyksho* Indictment ,r 43(c).

The GRU was also in contact through the Guccifer 2.0 persona with **HOM** a former Trump Campaign member **HOM**.¹⁵⁴ In early August 2016, **HOM** Twitter's suspension of 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, sadistic 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 1/19/15 Twitter Group Chat, Group ID 594242937858486276, @WikiLeaks et al. Assange also wrote that, "GOP will generate a lot opposition [sic], including through dumb moves. Hillary will do the same thing, but co-opt the liberal opposition and the GOP opposition. Hence biliary 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 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 prefab le [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 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 ,r 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. Assan e had access to the internet from the Ecuadorian Embassy in London, England. **Investigative Technique**

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

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

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

¹⁶² **Investigative Technique**

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 WikiLeaks email account. 6/29/16 Email, guccifer2@mail.com ~ (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 OM, @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 Muller-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 downloaded file's creation date same as shown on host computer. This would explain why the creation date on WikiLeaks's version of the files was still September 19, 2016. See SM2284941, 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 **Investigative Technique**

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 Technique¹⁷⁶

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**

¹⁷⁷ **Personal Privacy**

¹⁷⁸ **Personal Privacy**

¹⁷⁹ *Netyksho* Indictment ,r 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 **Personal Privacy**. 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 **Personal Privacy** including an email account belonging to Clinton aide **Personal Privacy**. 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 cloud-computing service **Personal Privacy**. On September 20, 2016, the GRU began to generate copies of the DNC data using **Personal Privacy** function designed to allow users to produce backups databases (referred to **Personal Privacy** 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**

them to **Personal Privacy** 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 **Investigative Technique** for vulnerabilities on of more than two dozen states. **Investigative Technique**

¹⁸⁵ Netyksho Indictment ,i 34; see also SM-2589105-HACK, serial 29 188 **Investigative Technique**

¹⁸⁶ Netyksho Indictment ,i 69.

¹⁸⁷ Netyksho Indictment ,i 69. **Investigative Technique**

¹⁸⁸ **Investigative Technique**

¹⁸⁹ **Investigative Technique**

¹⁹⁰ **Investigative Technique**

Similar **Investigative Technique** for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel a~ involved in voting technology. In August 2016, GRU officers targeted employees of , 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 2016. **Harm to Ongoing Matter**

1, **HOM**

a. Background

Harm to Ongoing Matter

¹⁹¹ Netyksho Indictment ,i 76. **Investigative Technique**

¹⁹² **Investigative Technique**

b. Contacts with the Campaign about WikiLeaks

Harm to Ongoing Matter

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** 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** Paul Manafort, who would later become campaign chairman ,

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 I 0/25/18 302, 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**. 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 **Harm to Ongoing Matter**.²⁰²

Harm to Ongoing Matter According to Gates, Manafort expressed excitement about the release **Harm to Ongoing Matter**.²⁰³ Manafort for his part, told the Office that shortly after the WikiLeaks's July 22 release, Manafort also spoke with Candidate Trump **Harm to Ongoing Matter**.²⁰⁴ **Harm to Ongoing Matter**.²⁰⁵ Manafort also **Harm to Ongoing Matter** 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 **Harm to Ongoing Matter**

²⁰¹ **Harm to Ongoing Matter**

²⁰² Cohen 9/18/18 302, at I 0. Harm to Ongoing Matter 200 **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 **Harm to Ongoing Matter** 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 b 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

c. **Harm to Ongoing Matter**

Harm to Ongoing Matter 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**

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; 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 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.

Harm to Ongoing Matter ²¹⁴ 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

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

Harm to Ongoing Matter

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 **HOM**

Malloch stated to investigators that beginning multiple Face Time 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

Harm to Ongoing Matter

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**

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

on October 7, 2016 four days after the Assange press conference **Harm to Ongoing Matter**, 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 Matter²⁴⁰ **Harm to Ongoing Matter**²⁴¹ **Harm to Ongoing Matter**²⁴²

Harm to Ongoing Matter²⁴³ **Harm to Ongoing Matter** Corsi said that, because he had no direct means of communicating with WikiLeaks, he told members of the news site WNO—who were participating on a conference call with him that day—to reach Assange immediately.²⁴⁴ Corsi claimed that the pressure was

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

²²⁸ **HOM**

²²⁸ **HOM**

²²⁸ **HOM**

²²⁸ **HOM**

²⁴⁴ In a later November 2018 interview, Corsi stated **HOM** that he believed Malloch was on the call but then focused 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 7²⁴⁸ **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 participant, or anyone who spoke Corsi that day, says 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 **Harm to Ongoing Matter** **Grand Jury**

²⁵¹ **Harm to Ongoing Matter** **Grand Jury**

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 pie 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~hbein to @WikiLeaks; see JF00587 (9/21/16 Messages, **PP** jabber.cryptoparty.is ~@jabber.cryptoparty.is ; **PP** 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 Floridabased 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

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** 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 **Grand Jury** 10/11/16 Email, Smith to **PP**

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 (bee: 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** 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.

Quick and Detailed Summaries created using dbi Technologies "Doc Tags" program.

Key Words : emails; Wikileaks; GRU; Clinton; campaign; dnc; account; trump; guccifer; dcleaks

Key Word : emails

Score : 263.82

Highlight : The investigation was unable to resolve Harm to Ongoing Matter WikiLeaks' release of stolen Podesta emails on October 7, 2016, the same day a video from years earlier was published of Trump using graphic language about women.

Key Word : Wikileaks

Score : 248.53

Highlight : 109 The GRU later released stolen Clinton Campaign and DNC documents through online personas, " DCLeaks XE "DCLeaks" " and "Guccifer XE "Guccifer" 2.0," and later through the organization WikiLeaks XE "WikiLeaks".

Key Word : GRU

Score : 243.43

Highlight : RUSSIAN HACKING XE "HACKING" AND DUMPING OPERATIONS Beginning in March 2016, units of the Russian XE "Russian" Federation' s Main Intelligence Directorate of the General Staff (GRU XE "GRU") hacked the computers XE "computers" and email accounts XE "email accounts" of organizations, employees, and volunteers supporting the Clinton XE "Clinton" Campaign XE "Clinton Campaign", including the email account XE "account" of campaign XE "campaign" chairman XE "campaign chairman" John Podesta.

Key Word : Clinton

Score : 174.61

Highlight : RUSSIAN HACKING XE "HACKING" AND DUMPING OPERATIONS Beginning in March 2016, units of the Russian XE "Russian" Federation' s Main Intelligence Directorate of the General Staff hacked the computers XE "computers" and email accounts XE "email accounts" of organizations, employees, and volunteers supporting the Clinton XE "Clinton" Campaign XE "Clinton Campaign", including the email account XE "account" of campaign XE "campaign" chairman XE "campaign chairman" John Podesta.

Key Word : campaign

Score : 150.39

Highlight : RUSSIAN HACKING XE "HACKING" AND DUMPING OPERATIONS Beginning in March 2016, units of the Russian XE "Russian" Federation' s Main Intelligence Directorate of the General Staff hacked the computers XE "computers" and email accounts XE "email accounts" of organizations, employees, and volunteers supporting the Clinton XE "Clinton" Campaign XE "Clinton Campaign", including the email account XE "account" of campaign XE "campaign" chairman XE "campaign chairman" John Podesta.

Key Word : dnc

Score : 127.45

Highlight : the GRU hacked into the computer networks of the Democratic Congressional Campaign XE "Campaign" Committee and the Democratic National Committee (DNC XE "DNC").

Key Word : account

Score : 126.18

Highlight : RUSSIAN HACKING XE "HACKING" AND DUMPING OPERATIONS Beginning in March 2016, units of the Russian XE "Russian" Federation' s Main Intelligence Directorate of the General Staff hacked the computers XE "computers" and email accounts XE "email accounts" of organizations, employees, and volunteers supporting the Clinton XE "Clinton" Campaign XE "Clinton Campaign", including the email account XE "account" of campaign XE "campaign" chairman XE "campaign chairman" John Podesta.

Key Word : trump

Score : 105.00

Highlight : The Trump campaign showed interest in the WikiLeaks releases and, in the summer and fall of 2016, Harm to Ongoing Matter After HOM Wikileaks' first Clinton-release HOM, the Trump Campaign stayed in contact HOM about WikiLeaks' activities.

Key Word : guccifer

Score : 90.49

Highlight : 109 The GRU later released stolen Clinton Campaign and DNC documents through online personas, " DCLeaks XE "DCLeaks" " and "Guccifer XE "Guccifer" 2.0," and later through the organization WikiLeaks XE "WikiLeaks".

Key Word : dcleaks

Score : 76.47

Highlight : 109 The GRU later released stolen Clinton Campaign and DNC documents through online personas, " DCLeaks XE "DCLeaks" " and "Guccifer XE "Guccifer" 2.0," and later through the organization WikiLeaks XE "WikiLeaks".

Index created using dbi Technologies "Document Indexer" program.

Access Hollywood, 74, 75
account, 36, 37, 38, 47, 51, 53, 54, 55, 56, 57, 58, 59, 61, 66, 74, 83, 87, 88
accounts, 36, 37, 38, 45, 47, 59, 65, 86
Administration, 61, 81
advisor, 45, 79, 81, 84
Agent, 39, 41, 43
alleging candidate Clinton, 77
ambitions, 54
AMS Panel, 41, 43
analyzing potential criticisms, 49
Anti-Doping Agency, 37
Apple operating system, 57, 85
Apple operating systems, 57
Assange, 51, 52, 56, 57, 58, 59, 60, 65, 70, 72, 74, 75, 76, 77
attachments, 45, 56, 57
Attorney, 67
authenticate, 83, 84
backup, 84
Bannon, 83
bitcoin, 37, 38, 45
bitcoin exchange platform, 38
blogger covering Florida, 49
breach, 47
business, 79, 83
campaign, 36, 38, 45, 51, 59, 65, 75, 77, 81, 83
Campaign, 36, 37, 38, 45, 49, 51, 57, 61, 63, 65, 68, 72, 74, 78, 79, 81, 83, 85, 87, 88
campaign chairman, 36, 38, 65, 87, 88
candidate Clinton, 51, 59
candidate Trum, 43, 49, 59, 65, 66, 68, 74, 81
candidate Trump, 43, 49, 59, 65, 66, 68, 74, 81
Candidate Trump, 66, 74
Caputo, 79, 80
Caputo accompanied Stone, 80
charge, 51
charges, 67, 86
chatroom, 77
Clinton, 36, 37, 38, 45, 49, 51, 52, 54, 57, 59, 60, 61, 65, 68, 74, 77, 78, 79, 81, 83, 84, 85, 87, 88, 89
Clinton campaign, 82
Clinton Campaign, 36, 37, 38, 45, 49, 51, 57, 61, 74, 78, 85, 87, 88, 89
Clinton Campaign-related communications, 38
Clinton emails, 51, 65, 68, 79, 81, 83, 85
Clovis, 83, 84, 85
CNN, 60
co-chairman Sam Clovis, 83
communicate, 41, 47, 51
communications, 38, 43, 51, 53, 55, 56, 57, 68, 75
computer network, 36, 39, 45, 49, 55, 61, 88
computer networks, 36, 45, 49, 55, 88
computers, 36, 37, 39, 41, 43, 61, 85, 87, 88
conducted large-scale spearphishing, 37
conducted pursuant, 69, 70
conference, 74, 75
Congress, 49, 67
conspiracy, 77
contacted multiple, 81
continued through, 63
contradictory recollections, 80
contributions, 84
controlled computers, 41
coordination, 53, 83
Corsi, 68, 69, 70, 72, 74, 75, 76, 85
counsel, 69
Counsel, 69
courage, 53
creation, 56, 57, 84, 85
crimes, 37
CrowdStrike Blog, 48
cyber operations, 37
dad tweets, 77
data pertaining, 43
DCCC, 36, 37, 39, 41, 43, 45, 49, 57, 86
DCCC employees, 39
DCLeaks, 36, 45, 46, 47, 49, 50, 51, 53, 55, 56, 59, 86, 87, 88, 89
Defending Julian Assange, 60
deleted Clinton, 81, 83, 84, 85
Deleted Clinton, 81
deleted Clinton emails, 81, 83, 84, 85
deleted Emails, 85
Democratic campaign, 59

Democratic Congressional Campaign, 36, 88
Democratic National Committee, 36, 48, 88
Democratic National Convention, 55
deputy, 65
detailed reports, 84
direct electronic communications, 75
direct message, 47, 53, 55, 77
direct messages, 47
Dissemination, 45, 63
District, 37, 67
DNC, 36, 37, 38, 39, 41, 43, 44, 45, 47, 49, 51, 53, 55, 56, 57, 58, 59, 60, 61, 65, 66, 86, 87, 88, 89
DNC documents, 36, 47, 53, 87, 88, 89
DNC mail server, 39
DNC network, 39, 41, 43, 47
DNC networks, 39, 41, 43
DNC Networks, 39
dnc Score, 88
DNC server hack, 47
document stating, 83
domain registration service, 46
Donald, 60, 66, 69, 75, 77
Donald Trump, 60, 69, 75, 77
DonaldJTrumpJr, 78
downloading, 85
eit, 53, 81
election, 36, 42, 43, 49, 51, 53, 59, 61, 63, 68, 83, 85, 86
Election, 72
elections, 37, 43, 61
Elections, 61
Ellen Nakashima, 57
email accounts, 36, 37, 38, 45, 59, 63, 85, 87, 88
email server, 46, 79, 81
emailed Smith, 81
emails, 38, 43, 45, 46, 49, 50, 51, 52, 53, 55, 56, 57, 58, 59, 63, 65, 66, 68, 72, 74, 75, 77, 79, 81, 83, 84, 85, 87
empire, 54
employees, 36, 38, 39, 43, 46, 63, 87, 88
encrypted account, 83
encrypted connection, 39
encrypted emails, 56
evidence, 51, 58, 59, 61, 76, 79, 81, 84, 85, 86
exfiltrating, 61
explanations, 66
exploiting, 61
Expressed Opposition, 51
Facebook, 47, 48
Facebook Message, 48
false statements, 65, 67
FBI, 44, 61, 63
file server, 43
file-transfer evidence, 58
financial documents, 53
financial information, 45
first Clinton-release HOM, 36, 88
first emails, 57
first set, 41, 74
Fishbein, 75, 77
Florida companies, 79
Floridabased Russian, 79
Flynn, 81, 82, 83, 84, 85
foreign, 65, 81
foreign services, 81
Forensic examination, 84
former deputy, 65
former DNC employee, 45
former executive vice, 66
former Trump Campaign, 51
fundraising files, 45
gain access, 37, 38, 63
Gates, 65, 66, 67, 68
German Hacker, 57
GOP, 46, 51, 52, 60
government, 57, 61, 63
grand jury, 37, 66
Grand Jury, 66, 67, 68, 70, 72, 76, 84
graphic language, 36, 87
GRU, 36, 37, 38, 39, 41, 43, 45, 46, 47, 49, 51, 53, 55, 56, 57, 59, 61, 63, 74, 85, 86, 87, 88, 89
GRU cyber unit, 36
GRU officers, 37, 38, 39, 41, 43, 47, 51, 53, 55, 56, 59, 61, 63, 86
GRU-controlled computers, 39, 41, 43, 61
Guccifer, 36, 45, 47, 48, 49, 50, 51, 53, 55, 56, 59, 86, 87, 88, 89
guilty, 65, 67
guilty plea, 67
Hacked Materials, 45, 63, 79
HACKING, 36
Harm, 36, 52, 63, 65, 66, 67, 68, 70, 72, 73, 74, 75, 76, 86, 88
hawkish liberal-interventionist appointees, 54

Henry Oknyansky, 79
 Highlight, 87, 88, 89
 Hillary Clinton, 49, 52, 65, 79
 HOM, 36, 51, 52, 63, 68, 70, 71, 73, 74, 75, 88
 Homeland Security, 61
 hoped Russia, 81
 host computer, 57
 Illinois State Board, 61
 Implantation, 39
 incident, 66
 Incorporation papers of KLS, 84
 indictment, 37
 Indictment, 37, 38, 42, 44, 45, 46, 48, 50, 54, 58, 62
 infected computers, 39, 43
 infiltrate, 40
 infra, 37, 66, 86
 initiated communications, 53
 intelligence sources, 81
 interference, 51, 81
 internal communications, 43, 57
 internal policy documents, 49
 interview, 58, 60, 65, 69, 70, 75, 76
 interviews, 67, 69, 70
 intrusion, 43, 48, 86
 investigation identified evidence, 61
 Investigative Technique, 37, 38, 39, 40, 41, 44, 46, 49, 50, 53, 54, 55, 56, 57, 58, 60, 61, 62, 64
 investigators, 72, 80
 investment advisor, 81
 Julian Assange, 51, 57, 65
 Key Words, 87
 KLS Research, 83, 84, 85
 KLS Research LLC, 83, 84
 LaGuardia Airport, 68
 landing, 45
 last-in-time DNC, 45
 launch, 47, 77
 leaked emails, 49, 50, 77
 leaked information, 58
 leaks, 53
 listed Jerome Corsi, 85
 local computer networks, 61
 local databases, 61
 local website, 61
 local websites, 61
 logs, 44, 77
 long-time Senate staffer, 81
 mail server, 43
 malicious activity, 61
 malicious software, 40, 63
 Malloch, 70, 72, 75
 malware, 36, 38, 39, 41, 63
 Manafort, 65, 66
 marry, 84
 Materials, 53, 57
 meeting, 79, 80, 81
 memorandum, 49
 memos, 84
 Michael, 66, 79, 81
 middle servers, 41
 Military Unit, 36, 37
 military units, 36
 Missing Hillary Clinton, 60
 Moscow, 47
 motivation, 79
 murder, 58
 National Security Advisor, 81
 network, 37, 38, 39, 43, 47, 61, 63
 networks, 36, 37, 39, 41
 Networks, 43
 Netyksho Indictment, 37, 38, 42, 44, 45, 46, 48, 50, 54, 58, 62, 64
 non-governmental organizations, 36
 officers, 37, 38, 39, 41, 43, 45, 47, 51, 53, 55, 56, 59, 61, 63, 86
 officials, 63
Oknyansky, 79, 80
 Ongoing Matter, 36, 52, 63, 65, 66, 67, 68, 70, 72, 73, 74, 75, 76, 86, 87, 88
 online personas, 36, 45, 86, 87, 88, 89
 opponent, 49
 opposition, 43, 49, 51, 52, 79
 opposition research, 43, 49, 79
 organization WikiLeaks, 36, 45, 87, 88, 89
 orsi, 68, 69, 75
 PAC, 77
 paid, 45, 80
 participant, 75
 parties, 46, 79, 85
 pending, 65
 persona, 47, 49, 50, 51, 53, 55, 56
 personal email account, 38, 45, 57
 Personal Privacy, 46, 48, 49, 50, 58, 59, 61
 Personal Privacy account, 61

personas, 49, 51, 55
 Peter Smith, 81, 84
 phrases, 47
 planning, 45, 68
 platform, 38
 plea agreement, 65, 66, 67
 Podesta email account, 57
 political science, 68
 politics, 49, 77, 81
 pool, 45
 posing, 51
 president, 66
 President, 85
 presidential campaign, 51, 83
 presidential election, 36, 49, 51
 press conference, 74
 Prince, 84, 85
 prior political jobs, 45
 private communication system, 51
 private messaging, 51, 53
 private network, 39, 41
 proffer agreement, 69, 70
 public prominence, 68
 publications, 77
 publishing, 53
 purposes, 83
 putintrump, 77
 Rare, 57
 Rasin, 79, 81
 reach Assange, 74
 received messages, 41
 refers, 40
 registered agent, 79
 registered Illinois voters, 61
 registrant, 45
 related GRU, 37
 released documents relating, 46
 released Podesta emails, 77
 releasing, 45, 49, 58, 59
 relevant items belonging, 61
 reporter, 47, 49, 50
 reporters, 47, 49, 50, 75
 reporters access, 49
 reporters Twitter, 47
 repository, 53
 Republican Party, 46
 request, 70, 81, 83
 resolve Harm, 36, 87
 response, 47, 55, 85
 restricted portion, 49
 resumed communications, 56
 Richard, 65
 RNC E-Mail, 47
 Roger Stone, 79
 routed funds, 38
 Russia, 36, 59, 77, 79, 81, 83, 85
 Russian, 36, 47, 57, 59, 60, 79, 81, 85
 RUSSIAN, 36, 87, 88
 Russian government, 57
 Russian hackers, 85
 RUSSIAN HACKING, 36, 87, 88
 Russians, 47, 59
 scanned state, 61
 sender, 37, 38, 45
 senior campaign, 77
 sensitive personal information, 43
 separately hacked computers, 37
 serials, 38, 57
 serve, 81
 servers, 41, 44, 61
 serving, 59
 sessions, 43, 66
 Seth Rich, 58
 shared file server, 39, 43
 shop, 79
 Similar Investigative Technique, 63
 Smith, 81, 82, 83, 84, 85, 86
 Smoking Gun, 47, 49
 snapshots, 60
 social media accounts, 37
 software vulnerabilities, 61
 solicited contributions, 84
 solicits information, 37
 solidify bernie supporters, 53
 spearphishing email, 37, 38, 57, 63
 spearphishing emails, 38, 63
 special counsel, 66
 Special Counsel, 69
 specialized malicious software, 36
 spoke Corsi, 75
 state boards, 37, 61
 Statements Dissembling, 57
 stating, 50, 70, 79, 81, 85
 stole documents, 43
 stolen data, 39
 stolen DCCC document, 51

stolen documents, 45, 51, 53, 55, 56
stolen emails, 45, 53, 57, 59, 75
stolen Podesta emails, 36, 56, 87
Stone, 79, 80, 81
sub, 36, 49, 50
subsequent communications, 55
superseding criminal information, 65
support, 53, 79, 83, 86
supra, 84, 85
Szobocsan, 82, 83, 84, 86
tape, 75
target Julian Assange, 77
targeting, 36, 37, 38, 42, 59, 61
Targeting Democrat-Linked Victims, 59
targeting individuals, 61
tech advisor, 84
Technique, 37, 38, 40, 44, 57, 61, 62, 64
televised interview, 65
television interview, 65
testimony, 65
third party, 40
tranches, 45, 57
trump, 53, 87, 88
Trump, 36, 43, 51, 59, 60, 63, 65, 66, 68, 69, 72,
74, 75, 77, 78, 79, 81, 83, 85, 86, 87, 88
Trump campaign, 36, 86, 88
Trump Campaign, 63, 68, 72, 79, 83, 85
Trump Organization, 66
Trump Tower Harm, 66
tweet, 75
Tweet, 58, 78
tweets, 76
Twitter, 47, 48, 51, 52, 53, 54, 55, 56, 57, 58, 77,
78
Twitter account, 47, 51, 53, 55, 56, 58
Twitter Group Chat, 52, 54
Ukrainian, 79
unique English words, 47
United States, 36, 37, 43, 46, 65, 68, 81
unlaunched site, 77
unsecured private email, 83
victim DCCC/DNC computers, 39
victims, 38, 45, 46, 59, 61
video, 36, 60, 74, 87
violation, 37, 67
volunteer, 49
voter registration software, 61
voting technology, 63
voting technology company, 63
VPN extends, 39
vulnerabilities, 61, 63
vulnerability, 61
Washington, 57, 69, 74
website, 45, 46, 47, 49, 50, 61, 75, 77
Western District, 37
Wikileaks, 50, 58, 78
WikiLeaks, 36, 45, 51, 52, 53, 54, 55, 56, 57, 58,
59, 60, 63, 65, 66, 68, 70, 72, 74, 75, 77, 78,
84, 85, 86, 87, 88, 89
WikiLeaks site, 56
witnesses, 66
WordPress blog, 47, 49
X-Agent, 39, 41, 43
York, 67, 84