Unit 26165 officers appear to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016.\textsuperscript{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 dceaks.com through a service that anonymized the registrant.\textsuperscript{137} Unit 26165 paid for the registration using a pool of bitcoin that it had mined.\textsuperscript{138} The dcleaks.com landing page pointed to different tranches of stolen documents, arranged by victim or subject matter. Other dceaks.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 passwod-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.\textsuperscript{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.\textsuperscript{140}

\textsuperscript{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.

\textsuperscript{137} Netyksho Indictment ¶ 35. Approximately a week before the registration of dceaks.com, the same actors attempted to register the website electionleaks.com using the same domain registration service.

\textsuperscript{138} See SM-2589105, serial 181; Netyksho Indictment ¶ 21(a).

\textsuperscript{139} Investigative Technique

\textsuperscript{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 First Vote, 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.\textsuperscript{141} The Facebook page was administered through a small number of preexisting GRU-controlled Facebook accounts.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{146}

---

\textsuperscript{141} Netyksho Indictment ¶ 38.

\textsuperscript{142} See, e.g., Facebook Account 100008825623541 (Alice Donovan).

\textsuperscript{143} 7/14/16 Facebook Message, ID 793058100795341 (DC Leaks) to ID Personal Privacy

\textsuperscript{144} See, e.g., 8/14/16 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&amp; enjoy ;).”

\textsuperscript{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.

\textsuperscript{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.\textsuperscript{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.”\textsuperscript{148} The GRU later sent the reporter a password and link to a locked portion of the dileaks.com website that contained an archive of emails stolen by Unit 26165 from a Clinton Campaign volunteer in March 2016.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{153}

---

\textsuperscript{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.

\textsuperscript{148} 6/27/16 Email, guccifer20@aol.fr to [Redacted] (subject “leaked emails”).

\textsuperscript{149} 6/27/16 Email, guccifer20@aol.fr to [Redacted] (subject “leaked emails”); see also 6/27/16 Email, guccifer20@aol.fr to [Redacted] (claiming DCLeaks was a “Wikileaks sub project”).

\textsuperscript{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.

\textsuperscript{151} Nettikso Indictment ¶ 43(a).

\textsuperscript{152} Nettikso Indictment ¶ 43(b).

\textsuperscript{153} Nettikso Indictment ¶ 43(c).
The GRU was also in contact through the Guccifer 2.0 persona with a former Trump Campaign member Harm to Ongoing Matter.

In early August 2016, Twitter’s suspension of the Guccifer 2.0 Twitter account. After it was reinstated, GRU officers posing as Guccifer 2.0 wrote via private message, “thank u for writing back ... do u find any[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 “what do u think of the info on the turnout model for the democrats entire presidential campaign.” responded, “pretty standard.”

The investigation did not identify evidence of other communications between 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 would [sic] then form a block to reign in their worst qualities.... With Hillary in charge, GOP will be pushing for her worst qualities, dems+media+neoliberals will be mute.... She’s a bright, well connected, sadistic sociopath.”

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

11/19/15 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 hillary has greater freedom to start wars than the GOP and has the will to do so.” Id.


44
[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.  

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.”

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.”

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 two [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.”

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,

---

158 3/14/16 Twitter DM, @WikiLeaks to @JP
159 6/14/16 Twitter DM, @dcleaks to @WikiLeaks.
160 Nat’l 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. \textbf{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.”\textsuperscript{163} The email contained an encrypted attachment with the name “wk dnc link1.txt.gpg.”\textsuperscript{164} Using the Guccifer 2.0 Twitter account, GRU officers sent WikiLeaks an encrypted file and instructions on how to open it.\textsuperscript{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.”\textsuperscript{166} On July 22, 2016, WikiLeaks released over 20,000 emails and other documents stolen from the DNC computer networks.\textsuperscript{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.”\textsuperscript{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.\textsuperscript{169} During subsequent communications, the

\textsuperscript{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 (The email appears to have been undelivered.)

\textsuperscript{164} See SM-2589105-DCLEAKS, serial 28 (analysis).

\textsuperscript{165} 6/27/16 Twitter DM, @Guccifer_2 to @WikiLeaks.

\textsuperscript{166} 7/18/16 Twitter DM, @Guccifer_2 & @WikiLeaks.


\textsuperscript{168} 9/15/16 Twitter DM, @dcleaks to @WikiLeaks.

\textsuperscript{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.\textsuperscript{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.\textsuperscript{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).\textsuperscript{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.\textsuperscript{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.pgp.”\textsuperscript{174} 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.\textsuperscript{175}

\textsuperscript{170} See SM-2589105-DCLEAKS, serial 28; 9/15/16 Twitter DM, @Guccifer_2 & @WikiLeaks.

\textsuperscript{171} See SM-2284941, serials 63 & 64.

\textsuperscript{172} 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.

\textsuperscript{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.

\textsuperscript{174} See 9/22/16 Email, dcleaksproject@gmail.com.

\textsuperscript{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

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;\textsuperscript{177} internal communications between Podesta and other high-ranking members of the Clinton Campaign;\textsuperscript{178} and correspondence related to the Clinton Foundation.\textsuperscript{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.”\textsuperscript{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

\textsuperscript{176} Investigative Technique

\textsuperscript{177} Personal Privacy

\textsuperscript{178} Personal Privacy

\textsuperscript{179} Netykhso Indictment ¶ 43.

\textsuperscript{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.”

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. 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.” 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, including an email account belonging to Clinton aide. 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. On September 20, 2016, the GRU began to generate copies of the DNC data using a function designed to allow users to produce backups of databases (referred to as “snapshots”). The GRU then stole those snapshots by moving

---

