

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

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

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

IRA employees posted derogatory information about a number of candidates in the 2016 U.S. presidential election. By early to mid-2016, IRA operations included supporting the Trump Campaign and disparaging candidate Hillary Clinton. The IRA made various expenditures to carry out those activities, including buying political advertisements on social media in the names of U.S. persons and entities. Some IRA employees, posing as U.S. persons and without revealing their Russian association, communicated electronically with individuals associated with the Trump Campaign and with other political activists to seek to coordinate political activities, including the staging of political rallies.<sup>5</sup> The investigation did not identify evidence that any U.S. persons knowingly or intentionally coordinated with the IRA’s interference operation.

By the end of the 2016 U.S. election, the IRA had the ability to reach millions of U.S. persons through their social media accounts. Multiple IRA-controlled Facebook groups and

---

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

<sup>3</sup> **Harm to Ongoing Matter**  
*see also* SM-2230634, serial 44 (analysis). The FBI case number cited here, and other FBI case numbers identified in the report, should be treated as law enforcement sensitive given the context. The report contains additional law enforcement sensitive information.

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

<sup>5</sup> *Internet Research Agency Indictment* ¶¶ 52, 54, 55(a), 56, 74; **Harm to Ongoing Matter**

Instagram accounts had hundreds of thousands of U.S. participants. IRA-controlled Twitter accounts separately had tens of thousands of followers, including multiple U.S. political figures who retweeted IRA-created content. In November 2017, a Facebook representative testified that Facebook had identified 470 IRA-controlled Facebook accounts that collectively made 80,000 posts between January 2015 and August 2017. Facebook estimated the IRA reached as many as 126 million persons through its Facebook accounts.<sup>6</sup> In January 2018, Twitter announced that it had identified 3,814 IRA-controlled Twitter accounts and notified approximately 1.4 million people Twitter believed may have been in contact with an IRA-controlled account.<sup>7</sup>

#### A. Structure of the Internet Research Agency

**Harm to Ongoing Matter**

<sup>8</sup> **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

<sup>10</sup>

The organization quickly grew. **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

<sup>11</sup>

<sup>12</sup>

The growth of the organization also led to a more detailed organizational structure. **Harm to Ongoing Matter**

---

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

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

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

<sup>9</sup> **Harm to Ongoing Matter**

<sup>10</sup> **Harm to Ongoing Matter**

<sup>11</sup> See SM-2230634, serial 86 **Harm to Ongoing Matter**

<sup>12</sup> **Harm to Ongoing Matter**

## Harm to Ongoing Matter

Two individuals headed the IRA's management: its general director, Mikhail Bystrov, and its executive director, Mikhail Burchik. Harm to Ongoing Matter

<sup>14</sup> Harm to Ongoing Matter

As early as the spring of 2014, the IRA began to hide its funding and activities. Harm to Ongoing Matter

The IRA's U.S. operations are part of a larger set of interlocking operations known as "Project Lakhta," Harm to Ongoing Matter

Harm to Ongoing Matter

## B. Funding and Oversight from Concord and Prigozhin

Until at least February 2018, Yevgeniy Viktorovich Prigozhin and two Concord companies funded the IRA. Prigozhin is a wealthy Russian businessman who served as the head of Concord.

<sup>13</sup> Harm to Ongoing Matter

<sup>14</sup> See, e.g., SM-2230634, serials 9, 113 & 180 Harm to Ongoing Matter

<sup>15</sup> Harm to Ongoing Matter

<sup>16</sup> Harm to Ongoing Matter

See SM-2230634, serials 131 & 204.

<sup>17</sup> Harm to Ongoing Matter

<sup>18</sup> Harm to Ongoing Matter

**Harm to Ongoing Matter**

**Prigozhin was sanctioned by the U.S. Treasury Department in December 2016,**<sup>19</sup>  
**Harm to Ongoing Matter**

<sup>20</sup> **Harm to Ongoing Matter**

<sup>1</sup> Numerous media sources have reported on Prigozhin's ties to Putin, and the two have appeared together in public photographs.<sup>22</sup>

**Harm to Ongoing Matter**

<sup>23</sup> **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

<sup>4</sup> **Harm to Ongoing Matter**

<sup>5</sup> **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

---

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

<sup>20</sup> **Harm to Ongoing Matter**

<sup>21</sup> **Harm to Ongoing Matter**

<sup>22</sup> See, e.g., Neil MacFarquhar, *Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as "Putin's Cook"*, New York Times (Feb. 16, 2018).

<sup>23</sup> **Harm to Ongoing Matter**

<sup>24</sup> **Harm to Ongoing Matter**

<sup>25</sup> **Harm to Ongoing Matter** see also SM-2230634, serial 113 **HOM**

**Harm to Ongoing Matter**



**Harm to Ongoing Matter**



<sup>26</sup> **Harm to Ongoing Matter**



<sup>27</sup>

**Harm to Ongoing Matter**



**Harm to Ongoing Matter**



<sup>28</sup>

**Harm to Ongoing Matter**



---

<sup>26</sup> **Harm to Ongoing Matter**

<sup>27</sup> **Harm to Ongoing Matter**

<sup>28</sup> The term “troll” refers to internet users—in this context, paid operatives—who post inflammatory or otherwise disruptive content on social media or other websites.

IRA employees were aware that Prigozhin was involved in the IRA's U.S. operations, [REDACTED]

**Harm to Ongoing Matter** [REDACTED]

<sup>29</sup> [REDACTED]

**Harm to Ongoing Matter** [REDACTED]

<sup>30</sup> In May

2016, IRA employees, claiming to be U.S. social activists and administrators of Facebook groups, recruited U.S. persons to hold signs (including one in front of the White House) that read "Happy 55th Birthday Dear Boss," as an homage to Prigozhin (whose 55th birthday was on June 1, 2016).<sup>31</sup>

**Harm to Ongoing Matter** [REDACTED]

<sup>32</sup> [REDACTED]

**Harm to Ongoing Matter** [REDACTED]

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

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

The IRA's U.S. operations sought to influence public opinion through online media and forums. By the spring of 2014, the IRA began to consolidate U.S. operations within a single general department, known internally as the "Translator" (Переводчик) department. [REDACTED]

**Harm to Ongoing Matter** [REDACTED]

[REDACTED] IRA subdivided the Translator Department into different responsibilities, ranging from operations on different social media platforms to analytics to

<sup>29</sup> **Investigative Technique** [REDACTED] See SM-2230634, serials 131 & 204.

<sup>30</sup> See SM-2230634, serial 156.

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

<sup>32</sup> **Harm to Ongoing Matter** [REDACTED]

[REDACTED] see also SM-2230634, serial 189. **Harm to Ongoing Matter** [REDACTED]

graphics and IT.

**Harm to Ongoing Matter**

<sup>33</sup> **Harm to  
Ongoing Matter**

<sup>34</sup>

**Harm to Ongoing Matter**

<sup>33</sup> **Harm to Ongoing Matter**

*See* SM-2230634, serial 205.

<sup>34</sup> *See* SM-2230634, serial 204 **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

**Harm to Ongoing Matter**

35

36

**Harm to Ongoing Matter**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] 37

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

Prior to traveling, Krylova and Bogacheva compiled itineraries and instructions for the trip.

**Harm to Ongoing Matter**

[REDACTED]

<sup>9</sup> **Harm to Ongoing Matter**

<sup>35</sup> **Harm to Ongoing Matter**

<sup>36</sup> **Harm to Ongoing Matter**

<sup>37</sup> **Harm to Ongoing Matter**

<sup>38</sup> See SM-2230634, serials 150 & 172 **Harm to Ongoing Matter**

<sup>39</sup> **Harm to Ongoing Matter**

**Harm to Ongoing Matter**  
**Harm to Ongoing Matter**

40

41

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

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

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

The IRA closely monitored the activity of its social media accounts.

**Harm to Ongoing Matter**

**Harm to Ongoing Matter**

40 **Harm to Ongoing Matter**

41 **Harm to Ongoing Matter**

42 **Harm to Ongoing Matter**

43 **Harm to Ongoing Matter**

44 *See, e.g.,* SM-2230634, serial 179 **Harm to Ongoing Matter**

<sup>45</sup> *See, e.g.,* Facebook ID 100011390466802 (Alex Anderson); Facebook ID 100009626173204 (Andrea Hansen); Facebook ID 100009728618427 (Gary Williams); Facebook ID 100013640043337 (Lakisha Richardson).

<sup>46</sup> The account claimed to be the “Unofficial Twitter of Tennessee Republicans” and made posts that appeared to be endorsements of the state political party. *See, e.g.,* @TEN\_GOP, 4/3/16 Tweet (“Tennessee GOP backs @realDonaldTrump period #makeAmericagreatagain #tngop #tennessee #gop”).

Harm to Ongoing Matter

Harm to Ongoing Matter

8

Harm to Ongoing Matter

By February 2016, internal IRA documents referred to support for the Trump Campaign and opposition to candidate Clinton.<sup>49</sup> For example, **HOM** directions to IRA operators **Harm to Ongoing Matter**

**Harm to Ongoing Matter** “Main idea: Use any opportunity to criticize Hillary [Clinton] and the rest (except Sanders and Trump - we support them).”<sup>50</sup> **Harm to Ongoing Matter**

The focus on the U.S. presidential campaign continued throughout 2016. In **HOM** 2016 internal **HOM** reviewing the IRA-controlled Facebook group “Secured Borders,” the

---

<sup>47</sup> **Harm to Ongoing Matter**

<sup>48</sup> See, e.g., SM-2230634 serial 131 **HOM**.

<sup>49</sup> The IRA posted content about the Clinton candidacy before Clinton officially announced her presidential campaign. IRA-controlled social media accounts criticized Clinton’s record as Secretary of State and promoted various critiques of her candidacy. The IRA also used other techniques. **Harm to Ongoing Matter**

**Harm to Ongoing Matter** See SM-2230634, serial 70.

<sup>50</sup> **Harm to Ongoing Matter**

author criticized the “lower number of posts dedicated to criticizing Hillary Clinton” and reminded the Facebook specialist “it is imperative to intensify criticizing Hillary Clinton.”<sup>51</sup>

IRA employees also acknowledged that their work focused on influencing the U.S. presidential election. **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

.<sup>52</sup>

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

Many IRA operations used Facebook accounts created and operated by its specialists. **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

<sup>53</sup>

**Harm to Ongoing Matter**

<sup>4</sup> IRA Facebook groups active during the 2016 campaign covered a range of political issues and included purported conservative

---

<sup>51</sup> **Harm to Ongoing Matter**

<sup>52</sup> **Harm to Ongoing Matter**

<sup>53</sup> **Harm to Ongoing Matter**

<sup>54</sup> **Harm to Ongoing Matter**

groups (with names such as “Being Patriotic,” “Stop All Immigrants,” “Secured Borders,” and “Tea Party News”), purported Black social justice groups (“Black Matters,” “Blacktivist,” and “Don’t Shoot Us”), LGBTQ groups (“LGBT United”), and religious groups (“United Muslims of America”).

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

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

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

IRA-purchased advertisements referencing candidate Trump largely supported his campaign. The first known IRA advertisement explicitly endorsing the Trump Campaign was purchased on April 19, 2016. The IRA bought an advertisement for its Instagram account “Tea Party News” asking U.S. persons to help them “make a patriotic team of young Trump supporters” by uploading photos with the hashtag “#KIDS4TRUMP.”<sup>60</sup> In subsequent months, the IRA purchased dozens of advertisements supporting the Trump Campaign, predominantly through the Facebook groups “Being Patriotic,” “Stop All Invaders,” and “Secured Borders.”

---

<sup>55</sup> 5/31/16 Facebook Message, ID 100009922908461 (Matt Skiber) to ID [REDACTED] 5/31/16 Facebook Message, ID 100009922908461 (Matt Skiber) to ID [REDACTED]  
**Personal Privacy**

<sup>56</sup> *Social Media Influence in the 2016 U.S. Election, Hearing Before the Senate Select Committee on Intelligence*, 115th Cong. 13 (11/1/17) (testimony of Colin Stretch, General Counsel of Facebook).

<sup>57</sup> 3/18/16 Facebook Advertisement ID 6045505152575.

<sup>58</sup> 4/6/16 Facebook Advertisement ID 6043740225319.

<sup>59</sup> See SM-2230634, serial 213 (documenting politically-oriented advertisements from the larger set provided by Facebook).

<sup>60</sup> 4/19/16 Facebook Advertisement ID 6045151094235.

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

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

A number of IRA employees assigned to the Translator Department served as Twitter specialists. **Harm to Ongoing Matter**

<sup>63</sup>

The IRA's Twitter operations involved two strategies. First, IRA specialists operated certain Twitter accounts to create individual U.S. personas, **Harm to Ongoing Matter**

<sup>4</sup> Separately, the IRA operated a network of automated Twitter accounts (commonly referred to as a bot network) that enabled the IRA to amplify existing content on Twitter.

##### *a. Individualized Accounts*

**Harm to Ongoing Matter**

<sup>65</sup> **Harm to Ongoing Matter**

---

<sup>61</sup> See Facebook ID 1479936895656747 (United Muslims of America); Facebook ID 1157233400960126 (Don't Shoot); Facebook ID 1601685693432389 (Being Patriotic); Facebook ID 757183957716200 (Secured Borders). **Harm to Ongoing Matter**

**Harm to Ongoing Matter**

**Harm to Ongoing Matter**

<sup>62</sup> *Social Media Influence in the 2016 U.S. Election, Hearing Before the Senate Select Committee on Intelligence*, 115th Cong. 13 (11/1/17) (testimony of Colin Stretch, General Counsel of Facebook).

<sup>63</sup> **Harm to Ongoing Matter**

<sup>64</sup> **Harm to Ongoing Matter**

<sup>65</sup> **Harm to Ongoing Matter**

## **Harm to Ongoing Matter**

66

The IRA operated individualized Twitter accounts similar to the operation of its Facebook accounts, by continuously posting original content to the accounts while also communicating with U.S. Twitter users directly (through public tweeting or Twitter's private messaging).

The IRA used many of these accounts to attempt to influence U.S. audiences on the election. Individualized accounts used to influence the U.S. presidential election included @TEN\_GOP (described above); @jenn\_abrams (claiming to be a Virginian Trump supporter with 70,000 followers); @Pamela\_Moore13 (claiming to be a Texan Trump supporter with 70,000 followers); and @America\_1st\_ (an anti-immigration persona with 24,000 followers).<sup>67</sup> In May 2016, the IRA created the Twitter account @march\_for\_trump, which promoted IRA-organized rallies in support of the Trump Campaign (described below).<sup>68</sup>

## **Harm to Ongoing Matter**

## **Harm to Ongoing Matter**

9

Using these accounts and others, the IRA provoked reactions from users and the media. Multiple IRA-posted tweets gained popularity.<sup>70</sup> U.S. media outlets also quoted tweets from IRA-controlled accounts and attributed them to the reactions of real U.S. persons.<sup>71</sup> Similarly, numerous high-

## **Harm to Ongoing Matter**

<sup>67</sup> Other individualized accounts included @MissouriNewsUS (an account with 3,800 followers that posted pro-Sanders and anti-Clinton material).

<sup>68</sup> See @march\_for\_trump, 5/30/16 Tweet (first post from account).

## **Harm to Ongoing Matter**

<sup>70</sup> For example, one IRA account tweeted, "To those people, who hate the Confederate flag. Did you know that the flag and the war wasn't about slavery, it was all about money." The tweet received over 40,000 responses. @Jenn\_Abrams 4/24/17 (2:37 p.m.) Tweet.

<sup>71</sup> Josephine Lukito & Chris Wells, *Most Major Outlets Have Used Russian Tweets as Sources for Partisan Opinion: Study*, Columbia Journalism Review (Mar. 8, 2018); see also *Twitter Steps Up to Explain #NewYorkValues to Ted Cruz*, Washington Post (Jan. 15, 2016) (citing IRA tweet); *People Are Slamming the CIA for Claiming Russia Tried to Help Donald Trump*, U.S. News & World Report (Dec. 12, 2016).

profile U.S. persons, including former Ambassador Michael McFaul,<sup>72</sup> Roger Stone,<sup>73</sup> Sean Hannity,<sup>74</sup> and Michael Flynn Jr.,<sup>75</sup> retweeted or responded to tweets posted to these IRA-controlled accounts. Multiple individuals affiliated with the Trump Campaign also promoted IRA tweets (discussed below).

*b. IRA Botnet Activities*

**Harm to Ongoing Matter**

<sup>6</sup>

**Harm to Ongoing Matter**

<sup>7</sup>

**Harm to Ongoing Matter**

<sup>78</sup>

In January 2018, Twitter publicly identified 3,814 Twitter accounts associated with the IRA.<sup>79</sup> According to Twitter, in the ten weeks before the 2016 U.S. presidential election, these accounts posted approximately 175,993 tweets, “approximately 8.4% of which were election-

---

<sup>72</sup> @McFaul 4/30/16 Tweet (responding to tweet by @Jenn\_Abrams).

<sup>73</sup> @RogerJStoneJr 5/30/16 Tweet (retweeting @Pamela\_Moore13); @RogerJStoneJr 4/26/16 Tweet (same).

<sup>74</sup> @seanhannity 6/21/17 Tweet (retweeting @Pamela\_Moore13).

<sup>75</sup> @mflynnJR 6/22/17 Tweet (“RT @Jenn\_Abrams: This is what happens when you add the voice over of an old documentary about mental illness onto video of SJWs. . .”).

<sup>76</sup> A botnet refers to a network of private computers or accounts controlled as a group to send specific automated messages. On the Twitter network, botnets can be used to promote and republish (“retweet”) specific tweets or hashtags in order for them to gain larger audiences.

<sup>77</sup> **Harm to Ongoing Matter**

<sup>78</sup> **Harm to Ongoing Matter**

<sup>79</sup> Eli Rosenberg, *Twitter to Tell 677,000 Users they Were Had by the Russians. Some Signs Show the Problem Continues*, Washington Post (Jan. 19, 2019).

related.”<sup>80</sup> Twitter also announced that it had notified approximately 1.4 million people who Twitter believed may have been in contact with an IRA-controlled account.<sup>81</sup>

### 5. U.S. Operations Involving Political Rallies

The IRA organized and promoted political rallies inside the United States while posing as U.S. grassroots activists. First, the IRA used one of its preexisting social media personas (Facebook groups and Twitter accounts, for example) to announce and promote the event. The IRA then sent a large number of direct messages to followers of its social media account asking them to attend the event. From those who responded with interest in attending, the IRA then sought a U.S. person to serve as the event’s coordinator. In most cases, the IRA account operator would tell the U.S. person that they personally could not attend the event due to some preexisting conflict or because they were somewhere else in the United States.<sup>82</sup> The IRA then further promoted the event by contacting U.S. media about the event and directing them to speak with the coordinator.<sup>83</sup> After the event, the IRA posted videos and photographs of the event to the IRA’s social media accounts.<sup>84</sup>

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

**Harm to Ongoing Matter**

[REDACTED]

---

<sup>80</sup> Twitter, “Update on Twitter’s Review of the 2016 US Election” (updated Jan. 31, 2018). Twitter also reported identifying 50,258 automated accounts connected to the Russian government, which tweeted more than a million times in the ten weeks before the election.

<sup>81</sup> Twitter, “Update on Twitter’s Review of the 2016 US Election” (updated Jan. 31, 2018).

<sup>82</sup> 8/20/16 Facebook Message, ID 100009922908461 (Matt Skiber) to ID **PP** [REDACTED].

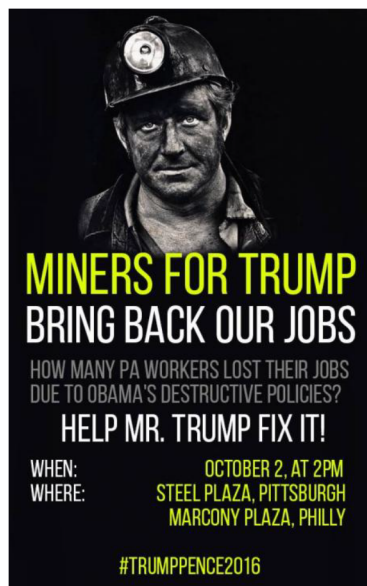
<sup>83</sup> See, e.g., 7/21/16 Email, joshmilton024@gmail.com to **PP** [REDACTED]; 7/21/16 Email, joshmilton024@gmail.com to **Personal Privacy** [REDACTED].

<sup>84</sup> @march\_for\_trump 6/25/16 Tweet (posting photos from rally outside Trump Tower).

<sup>85</sup> Instagram ID 2228012168 (Stand For Freedom) 11/3/15 Post (“Good evening buds! Well I am planning to organize a confederate rally [. . .] in Houston on the 14 of November and I want more people to attend.”).

**Harm to Ongoing Matter**





*IRA Poster for Pennsylvania Rallies organized by the IRA*

From June 2016 until the end of the presidential campaign, almost all of the U.S. rallies organized by the IRA focused on the U.S. election, often promoting the Trump Campaign and opposing the Clinton Campaign. Pro-Trump rallies included three in New York; a series of pro-Trump rallies in Florida in August 2016; and a series of pro-Trump rallies in October 2016 in Pennsylvania. The Florida rallies drew the attention of the Trump Campaign, which posted about the Miami rally on candidate Trump's Facebook account (as discussed below).<sup>86</sup>

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

**Harm to Ongoing Matter**

87

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

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

**Harm to Ongoing Matter**

**Harm to Ongoing Matter**

88

IRA employees frequently used **Investigative Technique** Twitter, Facebook, and Instagram to contact and recruit U.S. persons who followed the group. The IRA recruited U.S. persons from across the political spectrum. For example, the IRA targeted the family of **Personal Privacy** and a number of black social justice activists

<sup>86</sup> The pro-Trump rallies were organized through multiple Facebook, Twitter, and email accounts. See, e.g., Facebook ID 100009922908461 (Matt Skiber); Facebook ID 1601685693432389 (Being Patriotic); Twitter Account @march\_for\_trump; beingpatriotic@gmail.com. (Rallies were organized in New York on June 25, 2016; Florida on August 20, 2016; and Pennsylvania on October 2, 2016.)

<sup>87</sup> **Harm to Ongoing Matter**

<sup>88</sup> **Harm to Ongoing Matter**

while posing as a grassroots group called “Black Matters US.”<sup>89</sup> In February 2017, the persona “Black Fist” (purporting to want to teach African-Americans to protect themselves when contacted by law enforcement) hired a self-defense instructor in New York to offer classes sponsored by Black Fist. The IRA also recruited moderators of conservative social media groups to promote IRA-generated content,<sup>90</sup> as well as recruited individuals to perform political acts (such as walking around New York City dressed up as Santa Claus with a Trump mask).<sup>91</sup>

## **Harm to Ongoing Matter**

<sup>92</sup> **Harm to Ongoing Matter**

<sup>93</sup> **Harm to Ongoing Matter**

<sup>94</sup>

**HOM** as the IRA’s online audience became larger, the IRA tracked U.S. persons with whom they communicated and had successfully tasked (with tasks ranging from organizing rallies to taking pictures with certain political messages). **Harm to Ongoing Matter**

<sup>95</sup>

---

<sup>89</sup> 3/11/16 Facebook Advertisement ID 6045078289928, 5/6/16 Facebook Advertisement ID 6051652423528, 10/26/16 Facebook Advertisement ID 6055238604687; 10/27/16 Facebook Message, ID **Personal Privacy** & ID 100011698576461 (Taylor Brooks).

<sup>90</sup> 8/19/16 Facebook Message, ID 100009922908461 (Matt Skiber) to ID **PP**

<sup>91</sup> 12/8/16 Email, robot@craigslist.org to beingpatriotic@gmail.com (confirming Craigslist advertisement).

<sup>92</sup> 8/18-19/16 Twitter DMs, @march\_for\_trump & **PP**

<sup>93</sup> See, e.g., 11/11-27/16 Facebook Messages, ID 100011698576461 (Taylor Brooks) & ID **Personal Privacy** (arranging to pay for plane tickets and for a bull horn).

<sup>94</sup> See, e.g., 9/10/16 Facebook Message, ID 100009922908461 (Matt Skiber) & ID **Personal Privacy** (discussing payment for rally supplies); 8/18/16 Twitter DM, @march\_for\_trump to **PP** (discussing payment for construction materials).

<sup>95</sup> **Harm to Ongoing Matter**

## Harm to Ongoing Matter



### 7. Interactions and Contacts with the Trump Campaign

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

#### *a. Trump Campaign Promotion of IRA Political Materials*

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

- Posts from the IRA-controlled Twitter account @TEN\_GOP were cited or retweeted by multiple Trump Campaign officials and surrogates, including Donald J. Trump Jr.,<sup>96</sup> Eric

---

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

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

- A November 7, 2016 post from the IRA-controlled Twitter account @Pamela\_Moore13 was retweeted by Donald J. Trump Jr.<sup>103</sup>
- On September 19, 2017, President Trump's personal account @realDonaldTrump responded to a tweet from the IRA-controlled account @10\_gop (the backup account of @TEN\_GOP, which had already been deactivated by Twitter). The tweet read: "We love you, Mr. President!"<sup>104</sup>

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



*Screenshot of Trump Facebook Account (from Matt Skiber)*

<sup>97</sup> @EricTrump 10/20/16 Tweet ("RT @TEN\_GOP: BREAKING Hillary shuts down press conference when asked about DNC Operatives corruption & #VoterFraud #debatenight #TrumpB").

<sup>98</sup> @KellyannePolls 11/6/16 Tweet ("RT @TEN\_GOP: Mother of jailed sailor: 'Hold Hillary to same standards as my son on Classified info' #hillarysemail #WeinerGate.").

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

<sup>100</sup> @GenFlynn 11/7/16 (retweeting @TEN\_GOP post that included in part "@realDonaldTrump & @mike\_pence will be our next POTUS & VPOTUS.").

<sup>101</sup> @TEN\_GOP 10/11/16 Tweet ("North Carolina finds 2,214 voters over the age of 110!!").

<sup>102</sup> @TEN\_GOP 11/6/16 Tweet ("Mother of jailed sailor: 'Hold Hillary to same standards as my son on classified info #hillaryemail #WeinerGate.'").

<sup>103</sup> @DonaldJTrumpJr 11/7/16 Tweet ("RT @Pamela\_Moore13: Detroit residents speak out against the failed policies of Obama, Hillary & democrats . . .").

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

<sup>105</sup> 8/23/16 Facebook Message, ID 100009922908461 (Matt Skiber) to ID [REDACTED]

**Harm to Ongoing Matter**

106

***b. Contact with Trump Campaign Officials in Connection to Rallies***

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

\* \* \*

In sum, the investigation established that Russia interfered in the 2016 presidential election through the "active measures" social media campaign carried out by the IRA, an organization funded by Prigozhin and companies that he controlled. As explained further in Volume I, Section V.A, *infra*, the Office concluded (and a grand jury has alleged) that Prigozhin, his companies, and IRA employees violated U.S. law through these operations, principally by undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections.

<sup>106</sup> **Harm to Ongoing Matter**

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

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

### III. RUSSIAN HACKING AND DUMPING OPERATIONS

Beginning in March 2016, units of the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) hacked the computers and email accounts of organizations, employees, and volunteers supporting the Clinton Campaign, including the email account of campaign chairman John Podesta. Starting in April 2016, the GRU hacked into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). The GRU targeted hundreds of email accounts used by Clinton Campaign employees, advisors, and volunteers. In total, the GRU stole hundreds of thousands of documents from the compromised email accounts and networks.<sup>109</sup> 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**

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

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

##### 1. GRU Units Target the Clinton Campaign

Two military units of the GRU carried out the computer intrusions into the Clinton Campaign, DNC, and DCCC: Military Units 26165 and 74455.<sup>110</sup> 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.<sup>111</sup> 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.<sup>112</sup> **Investigative Technique** a bitcoin mining operation to

---

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

<sup>110</sup> *Netyksho* Indictment ¶ 1.

<sup>111</sup> 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.).

<sup>112</sup> 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.<sup>113</sup>

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.<sup>114</sup>

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.<sup>115</sup>

- Unit 26165 used **IT** to learn about **Investigative Technique** different Democratic websites, including democrats.org, hillaryclinton.com, dnc.org, and dccc.org. **Investigative Technique**  
[REDACTED] began before the GRU had obtained any credentials or gained access to these networks, indicating that the later DCCC and DNC intrusions were not crimes of opportunity but rather the result of targeting.<sup>116</sup>
- 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.<sup>117</sup>

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

---

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

<sup>113</sup> Bitcoin mining consists of unlocking new bitcoins by solving computational problems. **IT** 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.

<sup>114</sup> *Netyksho* Indictment ¶ 69.

<sup>115</sup> *Netyksho* Indictment ¶ 9.

<sup>116</sup> See SM-2589105, serials 144 & 495.

<sup>117</sup> **Investigative Technique**  
[REDACTED]

<sup>118</sup> **Investigative Technique**  
[REDACTED]

## 2. Intrusions into the DCCC and DNC Networks

### *a. Initial Access*

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

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

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

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

---

<sup>119</sup> **Investigative Technique**

<sup>120</sup> 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.

<sup>121</sup> **Investigative Technique**

SM-2589105-HACK, serial 5.

<sup>122</sup> **Investigative Technique**

M-2589105-HACK, serial 5.

<sup>123</sup> “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.

<sup>124</sup> **Investigative Technique**

<sup>125</sup> **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.<sup>126</sup> The first set of GRU-controlled computers, known by the GRU as “middle servers,” sent and received messages to and from malware on the DNC/DCCC networks. The middle servers, in turn, relayed messages to a second set of GRU-controlled computers, labeled internally by the GRU as an “AMS Panel.” The AMS Panel **Investigative Technique** served as a nerve center through which GRU officers monitored and directed the malware’s operations on the DNC/DCCC networks.<sup>127</sup>

The AMS Panel used to control X-Agent during the DCCC and DNC intrusions was housed on a leased computer located near **IT** Arizona.<sup>128</sup> **Investigative Technique**

<sup>129</sup>

**Investigative Technique**

**Investigative Technique**

---

<sup>126</sup> 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.

<sup>127</sup> *Netyksho* Indictment ¶ 25.

<sup>128</sup> *Netyksho* Indictment ¶ 24(c).

<sup>129</sup> *Netyksho* Indictment ¶ 24(b).

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

*c. Theft of Documents from DNC and DCCC Networks*

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

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

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

---

<sup>130</sup> *Netyksho* Indictment ¶¶ 27-29; **Investigative Technique**

<sup>131</sup> **Investigative Technique**

<sup>132</sup> **Investigative Technique**

<sup>133</sup> **Investigative Technique**

<sup>134</sup> **Investigative Technique**

SM-2589105-HACK, serial 5. **Investigative Technique**

<sup>135</sup> **Investigative Technique**

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

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

## **B. Dissemination of the Hacked Materials**

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

### **1. DCLeaks**

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

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

---

<sup>136</sup> *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.

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

<sup>138</sup> See SM-2589105, serial 181; *Netyksho* Indictment ¶ 21(a).

<sup>139</sup> **Investigative Technique**

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

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

GRU officers also used the DCLeaks Facebook account, the Twitter account @dcleaks\_, and the email account 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.<sup>143</sup> Similarly, on September 14, 2016, GRU officers sent reporters Twitter direct messages from @dcleaks\_, with a password to another non-public part of the dcleaks.com website.<sup>144</sup>

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

## 2. Guccifer 2.0

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

---

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).

<sup>141</sup> *Netyksho* Indictment ¶ 38.

<sup>142</sup> *See, e.g.*, Facebook Account 100008825623541 (Alice Donovan).

<sup>143</sup> 7/14/16 Facebook Message, ID 793058100795341 (DC Leaks) to ID **Personal Privacy**

<sup>144</sup> *See, e.g.*, 9/14/16 Twitter DM, @dcleaks\_ to **Personal Privacy**; 9/14/16 Twitter DM, @dcleaks\_ to **Personal Privacy**. The messages read: “Hi <https://t.co/QTvKUjQcOx> pass: KvFsg%\*14@gPgu&enjoy ;).”

<sup>145</sup> 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.

<sup>146</sup> *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.<sup>147</sup> Released documents included opposition research performed by the DNC (including a memorandum analyzing potential criticisms of candidate Trump), internal policy documents (such as recommendations on how to address politically sensitive issues), analyses of specific congressional races, and fundraising documents. Releases were organized around thematic issues, such as specific states (e.g., Florida and Pennsylvania) that were perceived as competitive in the 2016 U.S. presidential election.

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

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

---

<sup>147</sup> 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.

<sup>148</sup> 6/27/16 Email, guccifer20@aol.fr to **Personal Privacy** (subject “leaked emails”); **IT**.

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

<sup>150</sup> 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.

<sup>151</sup> *Netyksho* Indictment ¶ 43(a).

<sup>152</sup> *Netyksho* Indictment ¶ 43(b).

<sup>153</sup> *Netyksho* Indictment ¶ 43(c).

The GRU was also in contact through the Guccifer 2.0 persona with **HOM** a former Trump Campaign member **Harm to Ongoing Matter**

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

### 3. Use of WikiLeaks

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

#### *a. WikiLeaks's Expressed Opposition Toward the Clinton Campaign*

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

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

---

<sup>154</sup> **HOM**

<sup>155</sup> **Harm to Ongoing Matter**

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

<sup>157</sup> 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.<sup>158</sup>

***b. WikiLeaks’s First Contact with Guccifer 2.0 and DCLeaks***

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

**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.”<sup>160</sup>

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

***c. The GRU’s Transfer of Stolen Materials to WikiLeaks***

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

**Investigative Technique**

---

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

<sup>159</sup> 6/14/16 Twitter DM, @dcleaks\_ to @WikiLeaks.

<sup>160</sup> *Netyksho* Indictment ¶ 47(a).

<sup>161</sup> 7/6/16 Twitter DMs, @WikiLeaks & @guccifer\_2.

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

[REDACTED]

62

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

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

The same day, the Twitter account @guccifer\_2 sent @dcleaks\_ a direct message, which is the first known contact between the personas.<sup>169</sup> During subsequent communications, the

<sup>162</sup> **Investigative Technique**

[REDACTED]

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

<sup>164</sup> See SM-2589105-DCLEAKS, serial 28 (analysis).

<sup>165</sup> 6/27/16 Twitter DM, @Guccifer\_2 to @WikiLeaks.

<sup>166</sup> 7/18/16 Twitter DM, @Guccifer\_2 & @WikiLeaks.

<sup>167</sup> “DNC Email Archive,” WikiLeaks (Jul. 22, 2016), available at <https://wikileaks.org/dnc-emails>.

<sup>168</sup> 9/15/16 Twitter DM, @dcleaks\_ to @WikiLeaks.

<sup>169</sup> 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.<sup>170</sup>

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

Beginning on September 20, 2016, WikiLeaks and DCLeaks resumed communications in a brief exchange. On September 22, 2016, a DCLeaks email account [dcleaksproject@gmail.com](mailto: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."<sup>174</sup> **Investigative Technique** The email, however, bears a number of similarities to the July 14, 2016 email in which GRU officers used the Guccifer 2.0 persona to give WikiLeaks access to the archive of DNC files. On September 22, 2016 (the same day of DCLeaks' email to WikiLeaks), the Twitter account [@dcleaks](#) sent a single message to [@WikiLeaks](#) with the string of characters **Investigative Technique**

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

---

<sup>170</sup> See SM-2589105-DCLEAKS, serial 28; 9/15/16 Twitter DM, [@Guccifer\\_2](#) & [@WikiLeaks](#).

<sup>171</sup> See SM-2284941, serials 63 & 64 **Investigative Technique**

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

<sup>173</sup> 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.

<sup>174</sup> See 9/22/16 Email, [dcleaksproject@gmail.com](mailto:dcleaksproject@gmail.com) **IT**

<sup>175</sup> 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

176

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

### *d. WikiLeaks Statements Dissembling About the Source of Stolen Materials*

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

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

---

176 **Investigative Technique**

177 **Personal Privacy**

178 **Personal Privacy**

<sup>179</sup> *Netyksho* Indictment ¶ 43.

<sup>180</sup> @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."<sup>181</sup>

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

### C. Additional GRU Cyber Operations

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

#### 1. Summer and Fall 2016 Operations Targeting Democrat-Linked Victims

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

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

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

---

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

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

<sup>183</sup> "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).

<sup>184</sup> **Investigative Technique**

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

## 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.<sup>186</sup> The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations.<sup>187</sup> The GRU continued to target these victims through the elections in November 2016. While the investigation identified evidence that the GRU targeted these individuals and entities, the Office did not investigate further. The Office did not, for instance, obtain or examine servers or other relevant items belonging to these victims. The Office understands that the FBI, the U.S. Department of Homeland Security, and the states have separately investigated that activity.

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

GRU officers **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 websites of more than two dozen states. **Investigative Technique**

---

<sup>185</sup> *Netyksho* Indictment ¶ 34; *see also* SM-2589105-HACK, serial 29 **Investigative Technique**

<sup>186</sup> *Netyksho* Indictment ¶ 69.

<sup>187</sup> *Netyksho* Indictment ¶ 69; **Investigative Technique**

<sup>188</sup> **Investigative Technique**

<sup>189</sup> **Investigative Technique**

<sup>190</sup> **Investigative Technique**

## Investigative Technique

Similar **IT** for vulnerabilities continued through the election.

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

### D. Trump Campaign and the Dissemination of Hacked Materials

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

#### 1. **HOM**

##### *a. Background*

**Harm to Ongoing Matter**

<sup>191</sup> *Netyksho* Indictment ¶ 76; **Investigative Technique**

<sup>192</sup> **Investigative Technique**