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

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

C. Additional GRU Cyber Operations

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

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

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

Within approximately five hours of Trump’s statement, GRU officers targeted for the first time Clinton’s personal office. After candidate Trump’s remarks, Unit 26165 created and sent malicious links targeting 15 email accounts at the domain 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

---


\[183\] “Donald Trump on Russian & Missing Hillary Clinton Emails,” YouTube Channel C-SPAN, Posted 7/7/16, available at https://www.youtube.com/watch?v=3kxG8uU5sWU (starting at 0:41).

\[184\] Investigative Technique
them to 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.\textsuperscript{185}

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

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

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

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

\textsuperscript{185} Netyksho Indictment ¶ 34; see also SM-2589105-HACK, serial 29 \textit{Investigative Technique}.

\textsuperscript{186} Netyksho Indictment ¶ 69.

\textsuperscript{187} Netyksho Indictment ¶ 69; \textit{Investigative Technique}.

\textsuperscript{188} \textit{Investigative Technique}.

\textsuperscript{189} \textit{Investigative Technique}.

\textsuperscript{190} \textit{Investigative Technique}.
Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of [REDACTED], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election. 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. The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

D. Trump Campaign and the Dissemination of Hacked Materials

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

1. \[HOM\]

a. Background

\[Harm to Ongoing Matter\]

---

\[191\] Nemyko Indictment ¶ 76. \[Investigative Technique\]

\[192\] Investigative Technique