THE INFO OPS UNIT AT GRU, NOT THE TECHNICAL HACKING UNIT, HACKED THE STATE BOARDS OF ELECTION SERVERS

As I laid out a few weeks ago, I provided information to the FBI on issues related to the Mueller investigation, so I'm going to include disclosure statements on Mueller investigation posts from here on out. I will include the disclosure whether or not the stuff I shared with the FBI pertains to the subject of the post.

Yesterday, there was a big to-do on Twitter about a story (which subsequently got pulled) claiming that vote totals got changed as part of the Russian attack on the 2016 election. I don't care to engage the story — which I understand was very weak — directly. There are multiple ways for Russian efforts to have affected the outcome of the election, and the evidence increasingly supports a conclusion that that happened, without vote totals getting changed.

That said, given the focus on changing vote tallies, I want to note something about Mueller's GRU hacker indictment that has gotten almost no attention. Twelve men were indicted, from two different units of GRU, Units 26165 and 74455. The indictment describes the activities of each department in a way that *generally* suggests a division of labor, with Unit 26165 carrying out core hacking activities and Unit 74455 carrying out information operations. Here's what that breakdown looks like.

Unit 26165

Address: 20 Komsomolskiy Prospekt (this is the location spied on by the Dutch intelligence agency, AIVD).

Charged individuals:

- Viktor Netyksho: Commands Unit 26165
  - Boris Antonov: “Head of Department” that oversees spear-phishing targeting
    - Dmitriy Badin: “Assistant Head of Department” conducting spear-phishing targeting
    - Ivan Yermakov: works for Antonov, uses identities Kate Milton, Kames McMorgans, Karen Millen. Hacked at least two email accounts the contents of which were released by DCLeaks. Helped hack DNC emails server released through WikiLeaks.
    - Aleksey

Lukashev: Senior Lieutenant in Antonov's department. Uses identities Den Katenberg, Yuliana Martynova. Sent spear-phishing emails to Clinton campaign, including the one to John Podesta.

- Sergey Morgachev: Lieutenant Colonel who oversaw department that developed and managed X-Agent.
    - Nikolay Kozachek: Lieutenant Captain. Used monikers including "kazak" and "blablabla1234565." Developed, customized, and monitored X-Agent used to hack DCCC.
    - Pavel Yershov: Helped customize and text X-Agent before

deployment against DCCC.
- Artem Malyshev: Second Lieutenant in Morgachev's department. Used handles "djangomagicdev" and "realblatr." Monitored X-Agent implanted in DCCC and DNC servers.

Charged actions attributed to named defendants:

- ¶21-22: Spear-phishing targets
- ¶23-25: Hacking into DCCC
- ¶29-30: Stealing DCCC and DNC documents
- ¶33: Persistence in DCCC and DNC servers

Crimes charged to named defendants:

- Count One: CFAA
- Counts Two through Nine: Aggravated Identity Theft
- Count Ten: Conspiracy to Launder Money

Unit 74455

Address: 22 Korva Streett, Khimki (the Tower)

Charged individuals:

- Aleksandr Osadchuk: Colonel

and commanding officer of 74455, which assisted in release of stolen documents through DCLeaks, Guccifer 2.0, and the publication of anti-Clinton propaganda on social media.

- Aleksey Potemkin (!!): A supervisor in department responsible for administration of computer infrastructure used to assist in release in DCLeaks and Guccifer 2.0 documents.
- Anatoliy Kovalev: officer assigned to 74455 involved in hacks of State Boards of Election.

Charged actions attributed to named defendants:

- ¶38: Operating fictitious personas promoting DCLeaks
- ¶71-78: Hacking into State Boards of Election (SBOEs) and VR Systems

Crimes charged to named defendants:

- Count One: CFAA
- Counts Two through Nine: Aggravated Identity Theft
- Count Ten: Conspiracy to Launder Money
- Count Eleven: Conspiracy to Commit an Offense against

the US

Generally, the indictment describes Unit 26165 as being in charge of the technical hacking, including excruciating detail on what named officer played what role in phishing and malware deployment activities (probably thanks to the AIVD intelligence). The description of the information operations — running DC Leaks and Guccifer 2.0 and working with WikiLeaks — is less specific as to which officer did what, but the indictment clearly assigns those activities to Unit 74455. In any case, the indictment appears to suggest a division of labor, where Unit 26165 carries out the technical hacking and Unit 74455 carries out the information operations.

All 12 GRU officers are charged in Counts One through Ten.

Count Eleven, the ConFraudUs charge, is an outlier, however, in two ways. First, just Unit 74455 officers — Osadchuk and Kovalev — are charged in this operation. And aside from the indictment's description that Potemkin (!!) runs the infrastructure for Unit 74455, just the description of the phish of the State Boards of Election and VR Systems includes specific details about which Unit 74455 officer was involved in activities attributed to that unit.

All of which is to say that, for some reason, what is described as an information operations unit — Unit 74455 — conducted the hack of election infrastructure, not the technical hacking unit that carried out the other phishes of Democratic targets.

Perhaps the division of labor between these two units is not so clearcut as the indictment lays out. But if it is, then there may be an explanation why the information operations department would be hacking election infrastructure. Remember that in the days leading up to the election, Guccifer 2.0 —

according to the indictment, a Unit 74455 operation — predicted the Democrats might "rig the elections."

Hacks on SBOEs and election vendors would be an easy piece of evidence to point to to claim that Democrats had stolen the election. That is, it could be that these hacks (which, given that Illinois was targeted most aggressively, weren't going to alter the presidential election) may have been propaganda designed to undermine the Hillary win that never materialized.

Mind you, I still await the results of the investigation into whether there was a tie between the VR Systems hack and oddities in Durham County, NC on election day, something that would amount to voter suppression rather than altering vote tallies.

But it is at least possible that the attacks on our voting infrastructure were designed as propaganda, this time at least, rather than as an attempt to use the information obtained.