THE DECLASSIFIED RUSSIAN HACK REPORT

The Intelligence Community's report on Russia's tampering in the election is here.

What we see of it is uneven. I think the report is strongest on Russia's motive for tampering with the election, even if the report doesn't provide evidence. I think there are many weaknesses in the report's discussion of media. That raises concerns that the material on the actual hack — which we don't get in any detail at all — is as weak as the media section.

This will be a working thread.

The first 5 pages are front-matter and fluff, which means this is less than a 10 page report, plus a media annex which is problematic.

Scope

Here's how the report describes the scope of the assessment.

> It covers the motivation and scope of Moscow's intentions regarding US elections and Moscow's use of cyber tools and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the 2016 US presidential election and draws on our understanding of previous Russian influence operations. When we use the term "we" it refers to an assessment by all three agencies.

I checked with ODNI, and the classified report has the exact same conclusions as this one, suggesting the scope is the same. That seems to be a significant problem to me. At a minimum, it should address whether Shadow Brokers was part of the same campaign. But there are other, less obvious things that would need to be included that would not be under this scope, things that

I believe should be considered in the process of drawing conclusions.

The scope also includes this, which Director Clapper had already noted in yesterday's hearing.

> We did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election. The US Intelligence Community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze US political processes or US public opinion.

It's a bit of a cop-out, but a fair one: our nation's spooks should not be delving into electoral outcomes (aside from the way the FBI's Jim Comey was the most important player in this election after Hillary).

Sourcing

I'm fascinated by the entirety of the sourcing section. First, it doesn't even say that it is relying on private contractor reports, which it surely is.

> Many of the key judgments in this assessment rely on a body of reporting from multiple sources that are consistent with our understanding of Russian behavior.

Then there's this section that pretends the government doesn't have Putin and his associates lit up like Christmas trees.

> Insights into Russian efforts—including specific cyber operations—and Russian views of key US players derive from multiple corroborating sources. Some of our judgments about Kremlin preferences and intent are drawn from the behavior of Kremlin loyal
> political figures, state media, and pro-

> Kremlin social media actors, all of whom the Kremlin either directly uses to convey messages or who are answerable to the Kremlin.

On top of all the other problems with the media section, this use of media is tautological: a statement that because Russia has propaganda all its propaganda must be a clear representation of Russia's views.

> The Russian leadership invests significant resources in both foreign and domestic propaganda and places a premium on transmitting what it views as consistent, self-reinforcing narratives regarding its desires and redlines, whether on Ukraine, Syria, or relations with the United States.

Key Judgements

While it is nowhere near this bad elsewhere, check out how the IC conceives of Russia's efforts in terms of US exceptionalism, the "US-led liberal democratic order."

> Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the **US-led liberal democratic order**, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. [my emphasis]

I mean, Putin also wants to disrupt US backing of Saudi/Qatari regime change in Syria, and US backing for Neo-Nazis in Ukraine. But the IC pitches US hegemony as exclusively ponies and daisies.

Contrary to what you might read at other outlets, the assessment of Russia's motive describes Putin's animosity towards Clinton

before it addresses his fondness for Trump.

> Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.

In fact, the judgment that Putin affirmatively wanted Trump is broken out *largely because* the NSA has less confidence in this than the CIA and FBI.

> We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

That's especially interesting given the reference to what we know to be, in part, intercepts showing Putin and his buddies celebrating.

> Further information has come to light since Election Day that, when combined with Russian behavior since early November 2016, increases our confidence in our assessments of Russian motivations and goals.

That says that the folks who spend the most time reading SIGINT are the least convinced the SIGINT supports the case that Putin was hoping to get Trump elected.

Here's the key finding on the hack: that GRU not only hacked the targets but used the cut-outs to get the information to the outlets to publish.

> We assess with high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks.

We know the classified report describes the cut-outs that got the documents to Assange.

The one *new* disclosure in this document is that the IC now assesses the probes of state-related election outlets to be Russian, which they had never before done.

> Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.

I'll come back to this point.

I noted in my deep dive on the sanctions package that the sanctions apply to those who tamper in our allies' elections. This finding — that Russia wants to do more of this — is why the EO was written that way.

> We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes.

Russia's influence campaign

In addition to restating the top-line motives,

the section describing why Putin ordered this operation (and it does say that, explicitly) this section describes a few of the motives that the IC hasn't been as ready to leak to the press. It describes Putin's retaliation for Panama Papers and the Olympic doping scandal this way:

> Putin publicly pointed to the Panama Papers disclosure and the Olympic doping scandal as US-directed efforts to defame Russia, suggesting he sought to use disclosures to discredit the image of the United States and cast it as hypocritical.

Note how the passage *does not deny* that the US was behind Panama Papers (for which there is no public evidence) and the doping scandal (which would fit more squarely in the way the US wields its power). I assume the most compartmented version of this report explains whether we *did* have a role in Panama Papers.

The report also admits that Putin did this to retaliate for what protests he believes Clinton incited in Russia.

> Putin most likely wanted to discredit Secretary Clinton because he has publicly blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him.

Again, this passage is remarkably non-committal about whether the US did incite those protests.

The timing on the description of how Russia came to love the Donald is interesting — beginning in June.

> Beginning in June, Putin's public comments about the US presidential race avoided directly praising President-

> elect Trump,

In its description of Putin's desire to force an international ISIL coalition, the report doesn't address a number of things, most notably the reasons why we don't have an international coalition now. Again, this is a bullet point that I'm sure the most classified report has far more detail on.

> Moscow also saw the election of Presidentelect Trump as a way to achieve an international counterterrorism coalition against the Islamic State in Iraq and the Levant (ISIL).

Likewise, I wonder whether there's backup to this discussion of Putin's comfort in working with people who have business ties to Russia.

> Putin has had many positive experiences working with Western political leaders whose business interests made them more disposed to deal with Russia, such as former Italian Prime Minister Silvio Berlusconi and former German Chancellor Gerhard Schroeder.

How much did CIA lay out what Trump's business interests in Russia are?

The section on the actual hack is interesting. It starts by saying "Russian intelligence" got into the DNC in July 2015, which would refer to the FSB hack. Here's how it talks about the GRU hack(s).

> The General Staff Main Intelligence Directorate (GRU) probably began cyber operations aimed at the US election by March 2016. We assess that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political figures. By May, the GRU had exfiltrated large volumes of data from the DNC.

So:

- The report admits that they don't know when GRU started this. This is interesting for a slew of reasons, not least that it shows some uncertainty in the forensics.
- Note how it refers to "Democratic party officials and political figures," but never Podesta by name. It also doesn't name Colin Powell, though the follow-up language must include him too.
- Here, unlike in the JAR, the report says GRU exfiltrated a lot of data.

I'm not terrifically impressed by their paragraph on Guccifer 2.0, which is a problem, because this is one of the weakest parts of their argument.

> Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his likely Russian identity throughout the election. Press reporting suggests more than one person claiming to be Guccifer 2.0 interacted with journalists.

I'll come back to this. I just think it's weak in a number of places.

The DC Leaks passage is stronger.

> Content that we assess was taken from e-mail accounts targeted by the GRU in March 2016 appeared on DCLeaks.com

> starting in June.

Here's the passage on WikiLeaks.

> We assess with high confidence that the GRU relayed material it acquired from the DNC and senior Democratic officials to WikiLeaks. Moscow most likely chose WikiLeaks because of its selfproclaimed reputation for authenticity. Disclosures through WikiLeaks did not contain any evident forgeries.

The passage doesn't talk about cut-outs, but earlier leaks make it clear that's how it happened. I think the sentence "Moscow most likely chose WL" is either bullshit or not very smart.

Others have complained that this passage confirms there were no "obvious forgeries." The passage as a whole undermines some claims IC affiliates were saying in real time. So behind this paragraph, there's a whole lot of real-time assessments that were revisited. Indeed, several paragraphs later, the report makes the claim that forgeries are the MO for GRU.

> Such efforts have included releasing or altering personal data, defacing websites, or releasing emails.

I'm going to come back to the passage on WL and RT.

Note, the report includes the WADA hacking, even though the scope of this is supposed to be the election.

Again, I'm going to come back to the section on the info ops. I think it is weak, in part because it doesn't seem to distinguish genuinely held belief from outright propaganda. But this passage really gets to the core of the problem with it.

> RT's coverage of Secretary Clinton

> throughout the US presidential campaign was consistently negative and focused on her leaked e-mails and accused her of corruption, poor physical and mental health, and ties to Islamic extremism. Some Russian officials echoed Russian lines for the influence campaign that Secretary Clinton's election could lead to a war between the United States and Russia.

After all, you could say the same about most mainstream US outlets (some of which were ahead of RT on Hillary's health). There is almost nothing in the RT section that couldn't be said by a lot of US based outlets, some of which got bigger play. So how do you prove something is propaganda if it is doing what everyone else is doing? Moreover, much of what the passage points to depends on social media, and therefore algorithms built in Silicon Valley. Are they not a part of this propaganda? Also note, there's no discussion of Sputnik here, which was if anything more obvious in its opposition to Hillary. Why?

There's a long section from 2012 that deals with RT. I'll return to it when I return to the media section. It's really bad, though.

The report says it's not going to weigh in on whether Russia's efforts affected the election. But it does, here.

> We assess the Russian intelligence services would have seen their election influence campaign as at least a qualified success because of their perceived ability to impact public discussion.