ARGUMENT: THE DNC HACK ATTRIBUTION WAS A RESPONSE TO BRICK AND MORTAR EVENTS

Last week, ODNI and DHS released a statement widely viewed as attributing the hack and leak of DNC and other Democratic materials to Russia. The statement was actually a bit more nuanced than that:

Assertion 1: Russia compromised DNC and other political organizations

The statement starts with a comment that is spook speak for "we've proven this."

> The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations.

Mind you, this is the bit the IC has been confident of all along: they found hackers at the DNC and the hackers have all the attributes of two different Russian hacking groups.

Assertion 2: The leaking is consistent with stuff Russia has done elsewhere

The next move is the most interesting, in my opinion. The IC strongly suggests the leaking of those hacked files is Russia, but doesn't use the same spook speak confidence language.

> The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and

> WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts.

Here, the IC is *not* saying "we are confident Russia then handed all these files to WikiLeaks, as well as created two cover identities through which to leak them." Instead, they are saying Russia has done similar things before and has the motivation to do so here. As they have for months, the spooks still appear not to have the same level of proof tying the hacking to the leaking that would allow them to say "we are confident" for this assertion, at least not that they're willing to admit, which I find incredibly interesting.

Assertion 3: Russia is trying to interfere with the election

Having stated very confidently Russia did the hack and less confidently that it did the leak, the statement brings the nugget language: basically accusing Putin of masterminding the whole thing.

> These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

For my purposes here, I'm not interested in testing the truth of this statement — though I am a bit interested in how "influencing public opinion" is deemed to be "interfering with the US election," because it's something many people

don't seem to have thought through (nor have they thought through how it differs from the US' own information operations or PR involvement of other foreign powers in our elections).

Especially given this bit:

Assertion 4: Hackers operating through a Russian server hacked some state election websites, but that may not be the Russian state

The statement goes out of its way to note that the Russian-attributed activity *most* directly connected to the election, the voter rolls, may not actually be the Russian state, but instead just servers operated by a Russian company.

> Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government.

Remember, identity thieves have in the past stolen far more voter registration records for identity theft. It's certainly possible that's what went on here. More importantly, the IC appears to have nothing from collection on Russia they're willing to share to claim that this hacking is part of Putin's mastermind plot.

The rest of the statement goes on to talk about the ways (which I've talked about as well) that our localized system of elections makes it really hard to hack an election (though that also makes it really easy to botch an election or even to tamper with elections by disenfranchising select voters, which is what people should be far more concerned about, given that we know such efforts are effective and

ongoing).

The IC has long known this but chose to release this statement now

The reason I've broken this out into four parts — 1) we know Russia hacked the DNC, 2) the leaks of hacked material is consistent with stuff Russia has done in the past, 3) Putin is in charge, 4) Russia may not have hacked the state websites — is to call attention to the fact that the IC has been leaking assertions 1, 2, and 4 for months. The stated (leaked) reason to hold off on a formal attribution was the uncertain status of assertion 2: the IC doesn't yet know how the files got from the DNC hackers into Julian Assange's hands.

But the IC chose to release this statement without growing any more certain about assertion 2 and without solving assertion 4.

In my opinion, that means the IC released this statement to get to assertion 3. Putin is trying to "interfere" in our election by "influencing public opinion."

The release timing is more about kinetic events elsewhere than it is about IC certainty

So why release this statement now, when the IC doesn't seem to have gotten any more certain about assertion 2 or 4?

At the end of what I think is an overly pessimistic piece on America's inability to deter hacking, Jack Goldsmith considers the possibility that undeterred cyberattacks may be a response to brick and mortar conflict.

> Without robust defenses or effective deterrence, the United States can expect many more, and more harmful, cyber

> intrusions by adversaries who are asymmetrically empowered by the rise of digital networks. There is no end to the ways that they might spy in, steal from, or disrupt U.S. networks, public and private. That sounds bad, buts the implications are worse. Asymmetric offensive cyber operations by our adversaries can be an effective response to every element of U.S. foreign and military power. For all we know the Russian DNC hack is a response to sanctions for Ukraine and an attempt to win leverage in Syria. Imagine the United States wanted to do more—via sanctions, or through military operations, or in cyber—to slow Russian operations in Eastern Europe or Syria. The Russians could easily respond via cyber, where it appears to have an asymmetrical advantage. Indeed, the relatively tepid USG response to Russian aggression in Eastern Europe and Syria may be a result of USG worries about the implications of the DNC hack. In other words, the Russians may already be using cyber to deter the United States from seemingly unrelated foreign policy actions it might otherwise take.

Aside from his totally inappropriate use of "asymmetric" here — there's no lack of potential symmetry between the cyber capabilities of the US and Russia, just an emphasis of one tool over another — I agree with this passage. Indeed, I've been saying for a long time that the most obvious explanation for why Putin would do all this so blatantly is because in his view the US carried out a coup in Ukraine and is attempting regime change in Syria to choke Russia strategically.

And as Goldsmith argues, the US' weak spot is its vulnerability to cyber attacks, absolutely. That weakness is made worse, too, by continued US insistence on retaining access to all

potential offensive tools, even if they can be most dangerous against US targets if they ever, say, show up on an online sale (Goldsmith was curiously silent about the Shadow Brokers release here).

I suspect China, in particular, has done the same kind of mapping we have with Treasure Map, with a focus on having cyberattacks ready to launch that would neutralize us if we ever got into a hot war.

But Goldsmith doesn't consider the possibility that things may also work in the reverse way.

The US released this statement at a time when it was also making a big diplomatic push against Russia — proposing a ceasefire at the UN it knew Russia would veto, after having failed to negotiate a ceasefire with Russia directly because it asked for things (a no fly zone, basically) that Russia has neither the interest nor the legal necessity to agree to, because Russia is in Syria at the behest of the still-recognized government of the state, we're not. As it happens, the US is ratcheting up this effort at a time when our Saudi allies' activities in Yemen make it hard to make a principled stance against Russia, because we're implicated in Yemen in the same way Russia is in Syria.

More importantly, things are getting very very hot, with Russia moving missiles to Kaliningrad and threatening retaliation for any strikes on Syrian controlled territory.

So I would suggest the timing of this announcement — basically confirming the same certainty and uncertainty the IC has had for months, then using it to accuse Putin of trying to intervene directly in our country — is actually our response to more concrete events elsewhere, not the reverse (though there admittedly may be some chicken-and-egg stuff here, in that we may have held off on attribution in hope we could negotiate directly with Russia).

That is, both sides seem intent on ratcheting up the conflict between Russia and the US, and blaming Putin for interfering in our elections is one tool to do that.

If I'm right, the statement may have nothing to do with deterrence. Rather, it may have everything to do with escalation of other conflicts, providing a reason to pitch Russia's strategic moves elsewhere as a direct threat to the US. I'm not saying Russia isn't a dangerous adversary. I'm saying that the release of this statement will do nothing to prevent more hacks, but it will provide cause to claim the increasingly hot conflict with Russia directly threatens the US.