CYBERSECURITY

What Does the US Government Know About Russia and the DNC Hack?

By Susan Hennessey Monday, July 25, 2016, 12:03 PM

DayZero: Cybersecurity Law and Policy

Potentially unpleasant news for Jim Comey: We need you to intervene in the 2016 election again.

There is significant evidence that individuals acting at the direction of or on behalf of Russia—the degree of coordination is unclear—are attempting to use organizational doxing to influence the United States presidential election. As Jack noted this morning, this raises a number of scary questions regarding preserving the integrity of US election results. It is not entirely clear what is motivating the DNC document dumps or the apparent targeting of Hillary Clinton; some speculate the aim is to benefit Donald Trump, though a plausible goal might simply be to insert a degree of chaos into US politics. Understanding the ultimate goal of the hack and leaks, however, is not all that important to deciding how exactly we should respond. What is critical to mitigating the harm is sufficiently strong public attribution.

Defense One lays out the powerful, though not definitive, public evidence of Russian involvement. The New York Times offers a somewhat more tempered assessment. It is important to recognize that the strongest evidence regarding attribution was made public long before the most recent batch of emails was released:

- Director of National Intelligence James Clapper reported in May that the intelligence community had evidence that foreign governments were targeting campaigns.
- In June, Crowdstrike published its account, specifically naming Russian state actors as behind the DNC hack.
- While the Russians have long been known to use information and disinformation campaigns to influence foreign elections, there was initial skepticism regarding the degree of Crowdstrike's certainty. However, the discovery of incriminating metadata—first noticed by Matt Tait who tweets under @pwnallthethings—and other evidence quickly corroborated the Crowdstrike assessment.
- There are well-documented connections between Wikileaks—the chosen vehicle for the leak release—its founder Julian Assange, and the Russian state apparatus.

Paired with the technical indicators, the sum total of evidence is about as close to a smoking gun as can be expected where a sophisticated nation state is involved.

The leaked DNC emails have already cost Debbie Wasserman Schultz her chairmanship of the DNC. Julian Assange threatened in a June interview that the leaks would lead to Hillary Clinton's arrest. There is certainly nothing close to that in this batch of emails, and there is reason to doubt the validity of Assange's claim; he has wildly exaggerated about the content of leaks in the past and there are strategic reasons to lead major leaks with the most damaging information. But we are almost certain to see a number of leaks aimed at damaging Hillary Clinton over the coming weeks and months.

This means, put simply, that actors outside the US are using criminal means to influence the outcome of a US election. That's a problem.

The question before us now is how to construct a response to mitigate damage to our democratic institutions.

There is no exclusionary rule regarding media coverage of leaked or stolen information. The press cannot be asked to turn a blind eye out of patriotism to material released in the public domain. To the contrary, the strength of our system depends on an independent Fourth Estate that vigorously covers all information regarding political candidates. So Hillary is going to take whatever political hits she takes from the release of whatever this information contains.

However, it is crucial that the media not lose the thread that Russian state efforts to influence our democratic processes is the real story here. That story cannot vanish after an initial splash, and coverage of future leaked information should note the probable Russian involvement and involve analysis as to what the intended aims of leaking each new document might be. An informed public will need to evaluate new information situated in the context that it comes by means of a leak designed to manipulate the electorate's opinions.

This careful persistent context will depend on strong attribution. The more speculative the claim is—though it isn't all that speculative at this point—the less likely reporters are to view it as integral to coverage. Therefore, the US government would be wise to go on the record with as much definitive information regarding attribution as it can.

This may require overcoming some governmental inertia to not comment. The non-political elements of the executive branch are hesitant to weigh in on matters related to elections, and the blowback following FBI Director Comey's statement on the Clinton email investigation are a particularly fresh reminder of the perils. Beyond that, there is a fear that making even general claims of attribution may lead to calls for more concrete and sensitive evidence to be made public. In the early days following the hack and organizational doxing of Sony, the government went on the record that North Korea was behind the episode. After private industry experts questioned the strength of the technical evidence, the government was forced to disclose that it had additional information regarding DPRK involvement. Comey quelled doubts regarding the Sony attribution by stating that he had "a very high confidence about this attribution to North Korea, as does the entire intelligence community" and pointing to additional malware indicators. As a result, the government may be more hesitant to make public claims regarding nation state attribution because they do not want to risk compromising intelligence sources and methods in order to convince the public.

Here, however, the stakes are far higher.

Over the weekend, Dave Aitel argued that the "DNC hack and dump is what cyberwar looks like." There is a decent case that information systems surrounding our elections should qualify as "critical infrastructure" and that malicious nation states should recognize that interfering with these systems risks serious consequences. The absolute minimum response should be to make credible public attribution.

The US government is uniquely positioned to make the case for Russian attribution. The FBI and DHS have been working directly with the campaigns on cybersecurity, and the government has a combination of insight from both technical assessments of compromised networks and those intelligence information sources which the private sector lacks. And because the government has been historically very careful in stating conclusions regarding nation state involvement, it has a high degree of domestic and international credibility.

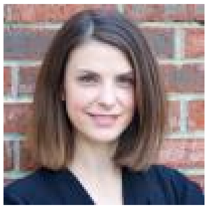
The best way to mitigate damage is to provide a clear US intelligence assessment as to whether there is Russian involvement and the degree of confidence. In May, Clapper was rather vague in noting that the IC was "aware that campaigns and related organizations and individuals are targeted by actors with a variety of motivations." With the implication to free and fair elections in the US, it is time for the FBI to get far more specific.

The Russian weapon is information. Our national values require that we not suppress information in the press, whatever its provenance. The solution is to fight fire with fire: our defense is more information. Protecting all sources and methods, the intelligence community and FBI should tell us who they think hacked and leaked the information. The rest of us can sort out why and whether that will matter on Election Day.

Topics: Cybersecurity, Campaign 2016

Tags: Russia

Susan Hennessey is Managing Editor of Lawfare and General Counsel of the Lawfare Institute. She is a Brookings Fellow in National Security Law. Prior to joining Brookings, Ms. Hennessey was an attorney in the Office of General Counsel of the



National Security Agency. She is a graduate of Harvard Law School and the University of California, Los Angeles.

@Susan_Hennessey

MORE ARTICLES ›

RELATED ARTICLES

Event Reminder: Cybersecurity in the Trump Administration: What Should We Expect?

Quinta Jurecic Thu, Feb 16, 2017, 10:24 AM

Cybersecurity in the Trump Administration: What Should We Expect?

Benjamin Wittes Mon, Feb 13, 2017, 4:17 PM

Revised Draft Trump EO on Cybersecurity

Paul Rosenzweig Thu, Feb 9, 2017, 12:22 PM

The Dangers of Walling Off America

Lisa Monaco Mon, Feb 6, 2017, 8:00 AM

What Does Russian Hacking of the U.S. Election Mean for the Rest of the World?

Arun Mohan Sukumar Wed, Feb 1, 2017, 9:18 AM

SUPPORT LAWFARE