CYBERSECURITY

Russia May Be Done with the U.S. Election, But We Aren't Done With Them

By **Susan Hennessey**, **Matt Tait** Friday, December 9, 2016, 12:21 PM

DayZero: Cybersecurity Law and Policy

This morning, counterterrorism and homeland security adviser Lisa Monaco announced that President Obama has ordered a "full review" of "hacking-related activity aimed at disrupting" the 2016 presidential election.

And the President is not alone in calling for continued scrutiny of Russian interference in the election; his announcement follows bipartisan calls from Congress for investigations into the matter.

Republican Senators, including Lindsay Graham and John McCain, have pledged to conduct subcommittee investigations; with Senator Graham telling CNN that he wants Putin to "pay a price." Meanwhile, Democrats in the House have introduced their own legislation to create a bipartisan commission to investigate election meddling by Russia, modeled after the 9/11 Commission.

The White House-directed review will be important to developing the relevant facts. But the bipartisan congressional interest in this issue is highly significant, especially because Congress is likely to play the largest role moving forward. In the aftermath of a bitterly partisan presidential election, it is easy to want to dismiss the "DNC Hack" and concern about foreign influence of election coverage as a mere partisan talking point. But the events which unfolded over the course of 2016 were not politics as usual. Both parties in Congress are rightly concerned about getting to the bottom of what occurred, primarily because they recognize that the attacks on the DNC and others was not really about helping Republicans at the expense of Democrats but instead about helping Russia at the expense of the United States. Recall, after all, that the hacks did not exclusively target Democrats, but also netted high-profile Republicans like Colin Powell, whose emails were also hacked and dumped online.

It is critical that we revisit the question of Russia's role now, not as a means to extract vengeance or to delegitimize the election result, but because there remains an urgent need for a response that establishes credible deterrence against future attacks on the United States and its allies which is currently lacking. The Obama administration has boasted that the U.S. "sent Russia a message" during the election, but evidently that message has fallen on deaf ears in Moscow, as the APT28 hacking group ramps up its efforts to undermine the democratic processes of our allies.

Take Germany, for example, as it prepares for its Bundestag elections in 2017. Here, Germany's BfV domestic intelligence agency is warning of a major campaign of Russian hacking, propaganda and disinformation aimed at destabilizing the government and influencing its election. (Original in German). BfV Director Dr. Hans-Georg Maaßen writes:

> In the political arena, we are increasingly having to deal with aggressive cyber-espionage. We see a potential threat to German government members, Bundestag delegates, and members of democratic political parties through cyber-operations. Information exfiltrated during cyber-attacks could emerge during an election campaign to discredit German politicians. The indications of attempts to influence the German Bundestag elections in the coming year are intensifying. We expect a further rise of cyber-attacks in the run up to the Bundestag election.

In the U.K, Alex Younger, Chief of the British Secret Intelligence Service (MI6), used a rare speech to say that his agency is seeing the same thing across Europe:

> This work has taken on a new edge when it comes to countering the increasingly dangerous phenomenon of hybrid warfare. The connectivity that is at the heart of globalisation can be exploited by States with hostile intent to further their aims deniably. They do this through means as varied as cyber-attacks, propaganda or subversion of democratic process. Our job is to give the government the information advantage; to shine a light on these activities and to help our country and our allies, in particular across Europe, build the resilience they need to protect themselves.

It is no surprise that Russia, having experienced astounding success at decisively influencing the media during the run up to the election, and with little, if any, visible repercussions for doing so, has now turned its attention to other countries in the West. Austria may have narrowly avoided electing the far-right and anti-EU Norbert Hofer this year, but in France, polls put Marine Le Pen only narrowly behind Francois Fillon for the Presidential election in May. In Germany, Chancellor Merkel is up for re-election shortly afterwards. These elections offer Vladimir Putin what may be his last, best chance to kill the European project outright.

This is why we can expect Russia to stay the course of using cyber attacks and disinformation strategies to disrupt Western democracies unless and until it is—as Graham puts it—forced to "pay a price." And considering what is at stake to gain and to lose, that price must be steep. The Obama White House struggled mightily with establishing an effective cyber deterrence strategy.

With only a few weeks remaining to conduct the investigative review, the Obama Administration can only hope to establish the relevant facts. It will likely fall to Congress to grapple with this, the most significant and consequential question of cyber deterrence the United States has yet faced: How should we respond to Russia's election aggression?

In calling for investigations, the current administration and Congress are laying the groundwork for a strong response—one capable of altering Russia's calculations as to whether this kind of activity is worthwhile in the long run. To impose a cost that genuinely outweighs the benefits—a cost which might include sanctions, counter-operations, and criminal indictments—it is necessary to gather firm evidence of both Russian responsibility and the extent of the activity in question. In part, this is because the United States and its allies will be called to justify their retaliation internationally.

The importance of developing irrefutable evidence is especially important in light of Trump's recalcitrance. Both as candidate and since as President-elect, Trump has repeatedly rejected intelligence community assessments on Russian malfeasance. The investigations will need to be robust and persuasive to overcome a likely desire for a muted, or nonexistent response from his administration.

Broadly speaking, the investigations will need to confirm three things. Firstly: Russia's role in hacking networks of the DNC, the DCCC, Clinton campaign staffers, and others and its role in releasing their private emails. Second: its role in targeting election infrastructure and related systems. Thirdly: Russia's role in spreading fake news and propaganda calculated to influence the American people.

Fortunately, much of the investigative work regarding the first two areas has already been done. In October, the Department of Homeland Security and Director of National Intelligence released a remarkably detailed joint statement stating that the intelligence community "is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations." The statement also reported "scanning and probing of [state] election-related systems" originating in Russia, but noted that there was insufficient evidence at the time to conclude that activity was actually directed by the Russian government. And media reports have extensively documented the Russian campaign. (See, for example. Thomas Rid's comprehensive account in Esquire.)

And since the election, Director of National Intelligence James Clapper has confirmed his confidence in the intelligence community assessment of Russia's interference during the election. In testimony before Congress, Clapper said "We gave considerable thought to diming out Russia", and emphasized that the intelligence community had waited "until we felt we had sufficient basis for it—and we did—both from a forensic and as well as other sources of intelligence that led us to that statement." In other words, the IC thought long and hard before making its assessment and now possesses multiple forms of proof.

It also appears that some significant evidence exists which has not yet been made public. Both during and after the election, Democrats on the congressional intelligence committees have called on President Obama to declassify evidence related to Russian election interference, in hopes of taking the case to the public. Last week, the Democratic members of the SSCI sent a terse public letter to the White House stating: "We believe there is additional information concerning the Russian government and the US election that should be declassified and released to the public. We

are conveying specifics through classified channels." While the letter was signed by Democrats, the significance should not be written off as mere partisanship. The Guardian reports "this is the first declassification request by eight senators in at least twelve years."

While members of Congress are entitled to see classified information, the President has final control over what information can be publicly released. Until noon on January 20, Barack Obama still decides what the American people are permitted to know about why the intelligence community believes Russia, and not a 400-pound hacker, assisted his successor in ascending to the highest office in the land. It is not clear how much of the current administration's report, which is expected to be concluded before Obama leaves office, will be unclassified. But the President should aim to declassify as much information as possible so that Congress can directly make the case to constituents about why they believe additional investigations are needed or why the matter should be put to rest. Considering the overwhelming national interests at stake, the current Administration should be forward-leaning and willing to accept a greater-than-usual degree of risk to sources and methods in order to make matters public.

Donald Trump won the presidency, and when he takes the oath of office there can be no dispute that he is fully and legitimately the President of the United States. We will never know the counterfactual of what would happen if Russia had not interfered, or the magnitude of their impact on the result. But for any number of other factors the outcome may also have been different. We will never know. But one thing is certain: Russia sought to dominate the media narrative in the run up to the US election, and are now seeking to do the same against our allies.

This fact is of profound significance to democracies. We need not agree on whether Russia changed the outcome to know that it is unacceptable for foreign governments to seek to directly interfere in democratic elections. Nor should we stand idly by when similar actions are taken against our allies in Europe.

The announcement of the executive review and congressional investigations are the first step towards figuring out exactly what happened. The next step—far more difficult and consequential—will be figuring out how to ensure it never happens again.

In MI6 Chief Younger's words "The risks at stake are profound and represent a fundamental threat to our sovereignty; they should be a concern to all those who share democratic values."

Topics: Cybersecurity, Transition 2016

Tags: DNC, 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 >

Matt Tait is the CEO and founder of Capital Alpha Security, a UK based security consultancy which focuses on research into software vulnerabilities, exploit mitigations and applied cryptography. Prior to founding Capital Alpha Security, Tait worked for Google Project Zero, was a principal security consultant for iSEC Partners, and NGS Secure, and worked as an information security specialist for GCHQ.

@pwnallthethings

MORE ARTICLES >

RELATED ARTICLES

Cybercrime Roundup: Searching and Seizing

Sarah Tate Chambers Wed, Feb 22, 2017, 3:02 PM

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

SUPPORT LAWFARE