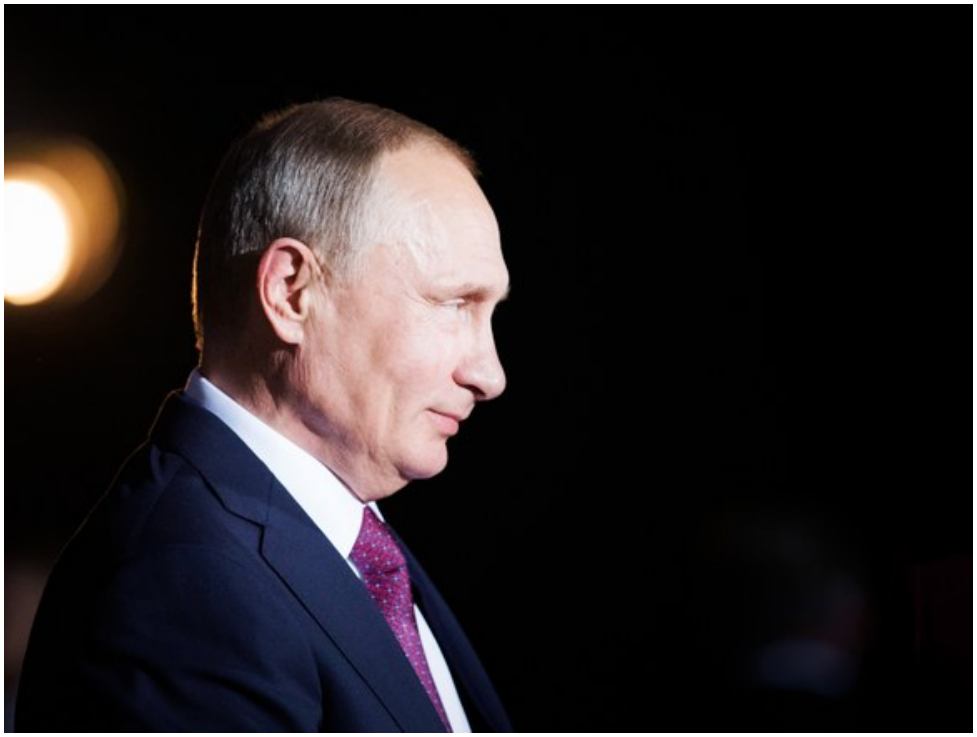
ANDY GREENBERG SECURITY 11.09.16 4:24 PM

TRUMP'S WIN SIGNALS OPEN SEASON FOR RUSSIA'S POLITICAL HACKERS



FLORIAN GAERTNER/GETTY IMAGES

YESTERDAY, AMERICA ELECTED as president the apparently preferred candidate of Russia's intelligence agencies. After a campaign season marred by the influence of hackers, including some widely believed to be on Vladimir Putin's payroll, that outcome means more than a mandate for Trump and his coalition. For Russia, it will also be taken as a win for the chaos-injecting tactics of political hacks and leaks that the country's operatives used to meddle in America's election—and an incentive to try them elsewhere.

Following Donald Trump's presidential win, and even in the weeks leading up to it, cybersecurity and foreign-policy watchers have warned that Russia's government-sponsored hackers would be emboldened by the success of the recent string of intrusions and data dumps, including the hacks of the Democratic National Committee and the Democratic Congressional Campaign Committee. Security firms that analyzed the breaches, and US intelligence agencies, have both linked those attacks to the Kremlin. That Russia perceives those operations as successful, experts say, will only encourage similar hacks aimed at shifting elections and sowing distrust

of political processes in Western democracies, particularly those in Europe. “What they’ll learn from this is, ‘We did it, we got away with it, we got the outcome we wanted,’” says James Lewis, a cybersecurity-focused fellow with the Center for Strategic and International Studies. “This will only increase their desire to intervene.”

Fancy Bears Hit Europe

In fact, those interventions and intrusions are already underway. Since this summer’s breaches of the Democratic party, at least a dozen European organizations have also been targeted by the state-linked Russian hacker group known as Fancy Bear, or APT28, according to Dmitri Alperovitch, the chief technology officer of the security firm Crowdstrike, which identified Russia as the culprit behind the DNC hack in July. Several of those attempts have been successful, he says, and multiple American targets of the group have also been hacked but have yet to publicly reveal that they were compromised. A report out today from security firm Trend Micro confirms the group has continued to hit “various governments and embassies around the world” in just the last weeks. “They’ve continued their attempted intrusions of political entities pretty much unabated,” Alperovitch says.[1]

Even before Trump’s win, Alperovitch says, he believes Russia considered Fancy Bear’s hacking operations a significant achievement. He points to the uncertainty and doubt the hacker group was able to instill in American electoral politics, with everyone from Bernie Sanders supporters to rightwing media to Donald Trump himself making arguments that the system was “rigged” in favor of Hillary Clinton. “I think they’ve gotten medals already,” Alperovitch told WIRED in an interview before Tuesday’s election. “They’ve had success beyond their wildest dreams.”

Alperovitch adds that he’s met with senior government officials across Europe who fear that the Kremlin’s ability to influence American electoral politics presages attacks aimed at upcoming elections in France and Germany, as well as the UK’s parliamentary vote on Brexit. “They’re concerned that the blueprint used now against the US will be used against them in upcoming election cycles,” says Alperovitch. “They’re concerned that the precedent that’s been set is that you can do this against the US, and if so, that they’ll be walked all over by Russia.”

Russia’s state-sponsored hackers targeting Western political institutions is, to be clear, hardly new. In just the past few years, hackers believed to be based in Russia have breached the White House and the State Department, for instance, even leading

at one point last year to a temporary shutdown of the State Department's email systems.

But compared with those silent espionage intrusions, the recent hacks have been increasingly brazen, with hacked emails and documents made public in order to influence American media and public opinion. By the time of the breach of the World Anti-Doping Agency in September, designed to implicate US athletes in suspect behavior, the hackers no longer even sought to hide their connection to Russia. The hackers published the medical files of high-profile US Olympians on the site Fancybears.net, and adorned them with GIFs of dancing bears.

No Clear Remedy

Those increasingly common techniques have blended hacking and propaganda in a way that American intelligence agencies haven't in kind, says Thomas Rid, a cybersecurity-focused professor in the department of War Studies at King's College London and author of *Rise of the Machines*. And Russia's information operations only become more effective as Western democracies become increasingly polarized. Beyond Trump, Rid points to Brexit, the rise of the nationalist, nativist French party National Front, and a recent German poll in which respondents at both the extreme left and right said they had more trust in Putin than in Angela Merkel. "The ground is becoming more fertile for Russia's influence operations," says Rid. "Trump is the embodiment of that."

Russia's shift to bold, barely covert hacking operations has also no doubt stemmed partly from a sense of impunity. American intelligence agencies took months to publicly name the Russian government as the source of the DNC hack that came to light in July. Even then, the response has been murky: Despite Vice President Joe Biden's assurances that the US would be "sending a message" to Putin intended to have "maximum impact," it's not clear if or how that counterattack happened.

Trump's win may now delay America's response or reduce its efficacy, says the CSIS's Lewis. Even if the Obama administration carries out its response before Trump's inauguration, Putin may doubt that any policy of deterrence would carry over to Trump's administration—particularly given the fondness for Putin that Trump expressed on the campaign trail, his weak support for NATO, and the doubts Trump has publicly cast on attributing the DNC hack to Russia. After January, America's account of grievances against Russia's hackers could be wiped clean. "For Trump,

there will be a before and an after" the election, says Lewis. "If they do something that hurts him, he'll respond. But if it happened before the election, it's over."

All of that means Russia's hacking spree may have just begun. Expect Fancy Bear and its habit of digitally disemboweling Western political targets to be an unwelcome fixture of Trump's first term—and beyond.

[1]*Correction 11/11/16 10:00am EST: An earlier version of this story mistakenly called Dmitri Alperovitch Crowdstrike's CEO, not its CTO.*