Research Memo

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Russia and the 2016 Presidential Election

By Pasi Eronen

August 2016

For a decade, Russian President Vladimir Putin has been working to overturn pillars of the post-war political and economic order in Europe. Among attacks aimed at bolstering Moscow's strategic position, Russian intelligence agencies have funded extremist political parties that challenge the status quo, spread propagandized news to incite Russian-speaking immigrants in Europe,[1] and invaded and annexed territory belonging to Russia's neighbors.[2] Now, the Kremlin is the primary suspect in the theft of some 20,000 emails from the Democratic National Committee (DNC) and their release to WikiLeaks, which divulged them just before the party's convention.[3] While the U.S. is hardly a new target for Russian espionage, the move – if proven to be carried out by Moscow – would reflect a serious escalation of Putin's offensive against the West.

Over the last year, experts have accused Russia of a broad hacking campaign in Washington involving more than 100 entities and individuals.[4] The DNC breach was believed to be a search for damaging material that the Democratic Party had disinterred on Republican presidential nominee Donald Trump, according to CrowdStrike, the private cyber-security firm that investigated the attack.[5] Before that, however, Russia broke into President Barack Obama's unclassified email,[6] along with the email servers of the State Department and the Joint Chiefs of Staff.[7] According to CrowdStrike, Russia hacked the Clinton Foundation and several think tanks associated with

1. Adam Taylor, "An alled rape sparked tensions between Russia and German. Now police say it was fabricated," *The Washington Post*, January 29, 2016. (https://www.washingtonpost.com/news/worldviews/wp/2016/01/29/an-alleged-rape-sparked-tensions-between-russia-and-germany-now-police-say-it-was-fabricated/)
2. Pasi Eronen, "Russian Hybrid Warfare: How to Confront a New Challenge to the West," *Foundation for Defense of Democracies*, June 2016. (http://www.defenddemocracy.org/content/uploads/documents/Russian_Hybrid_Warfare.pdf)
3. Max Fisher, "Why Security Experts Think Believe Russia Was Behind the D.N.C. Breach," *The New York Times*, July 26, 2016. (http://www.nytimes.com/2016/07/27/world/europe/russia-dnc-hack-emails.html)
4. Eric Lichtblau and Eric Schmitt, "Hack of Democrats' Accounts Was Wider Than Believed, Officials Say," *The New York Times,* August 11, 2016. (http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html)
5. Tal Kopan, "Russian hackers stole Dems' Trump files, firm says," *CNN,* June 14, 2016. (http://www.cnn.com/2016/06/14/politics/democratic-national-committee-breach-russians-donald-trump/)
6. Michael S. Schmidt and David E. Sanger, "Russian Hackers Read Obama's Unclassified Emails, Officials Say," *The New York Times*, April 25, 2015. (http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html)
7. Danny Yadron, "Three Months Later, State Department Hasn't Rooted Out Hackers," *The Wall Street Journal*, February 19, 2015. (http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453); Shane Harris, "Exclusive: Russian Hackers Target The Pentagon," *The Daily Beast*, July 18, 2015. (http://www.thedailybeast.com/articles/2015/07/18/russian-hackers-target-the-pentagon.html); Barbara Starr, "Official: Russia suspected in Joint Chiefs email server intrusion," *CNN*, August 7, 2015. (http://www.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/)

Pasi Eronen is the project researcher for the Foundation for Defense of Democracies' Russia project, where his research focuses on economic warfare and the nexus with cyberwarfare.

Democratic nominee Hillary Clinton and the Democratic Party.[8] In addition, Russian hackers are believed to have hacked the personal email accounts of scores of consultants, lawyers, and political operatives working for Clinton or her party.[9]

The release of DNC emails to WikiLeaks, if proven, suggests that Russia has shifted from the traditional espionage conducted by all major nations to concrete political operations with the potential of influencing elections. Indeed, according to retired senior U.S. military and intelligence officers, Moscow or some other foreign power could or may already be preparing to sway the November 8 presidential election itself.[10]

The foreign policy and intelligence communities are conflicted on how to respond. President Obama has ordered an FBI investigation, but meanwhile is speaking circumspectly. Even if the probe shows Russia is responsible, Obama said on August 2 that it would not significantly change his already-sour appraisal of "a tough, difficult relationship that we have with Russia right now."[11] He appears to be cautious about imposing new sanctions against Russia, given the danger of further complicating other strategic priorities such as Syrian policy, and the difficulty of holding together a united Western approach on sanctions. But some intelligence and military experts have urged a deterrent response.[12]

In taking this battle to the United States, Putin appears to believe he is responding in kind – he is convinced that the U.S. masterminded the 2014 overthrow of the pro-Moscow Ukrainian President Viktor Yanukovych.[13] He also alleges that the Democratic nominee for president, Hillary Clinton, fomented and paid for large 2011 protests challenging his rule while she was secretary of state. Putin said at the time, "She set the tone for some actors in our country and gave them a signal. They heard the signal and with the support of the U.S. State Department began active work."[14]

As practiced by Russia, cyberwarfare is a broader concept than conventionally understood. During the initial days after seizing Crimea in March 2014, Russia sought first to sever the local population and regionally-based military units from mainland Ukraine. It attacked communications infrastructure such as fiber connections between Crimea and the mainland Ukraine, captured the peninsula's sole Internet exchange point, and jammed radio connections.[15] At the same time, Moscow carried out similar jamming in Eastern Ukraine, in this case for

8. Michael Riley and Jordan Robertson, "Clinton Foundation Said to be Breached by Russian Hackers," *Bloomberg,* June 22, 2016. (https://www.bloomberg.com/news/articles/2016-06-22/clinton-foundation-said-to-be-breached-by-russian-hackers)
9. Eric Lichtblau and Eric Schmitt, "Hack of Democrats' Accounts Was Wider Than Believed, Officials Say," *The New York Times,* August 11, 2016. (http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html)
10. Aspen Institute Homeland Security Group, Statement, July 28, 2016. (http://www.prnewswire.com/news-releases/members-of-the-aspen-institute-homeland-security-group-issue-statement-on-dnc-hack-300306004.html)
11. The White House, "Remarks by President Obama and Prime Minister Lee of Singapore in Joint Press Conference," August 2, 2016. (https://www.whitehouse.gov/the-press-office/2016/08/02/remarks-president-obama-and-prime-minister-lee-singapore-joint-press)
12. Aspen Institute Homeland Security Group, Statement, July 28, 2016. (http://www.prnewswire.com/news-releases/members-of-the-aspen-institute-homeland-security-group-issue-statement-on-dnc-hack-300306004.html)
13. "Putin in film on Crimea: US masterminds behind Ukraine coup, helped train radicals," *RT* (Russia), March 15, 2015. (https://www.rt.com/news/240921-us-masterminds-ukraine-putin/)
14. David M. Herszenhorn and Ellen Barry, "Putin Contents Clinton Incited Unrest Over Vote," *The New York Times*, December 8, 2011. (http://www.nytimes.com/2011/12/09/world/europe/putin-accuses-clinton-of-instigating-russian-protests.html)
15. Keir Giles, "Russia and Its Neighbours: Old Attitudes, New Capabilities," *Cyber War in Perspective: Russian Aggression against Ukraine*, Ed. Kenneth Geers, (NATO Cooperative Cyber Defence Centre of Excellence, 2015), pages 19-28; Piret Pernik, "Is All Quiet on the Cyber Front in the Ukrainian Crisis?" *International Centre for Defense and Security* (Estonia), March 7, 2014. (http://www.icds.ee/et/blogi/artikkel/is-all-quiet-on-the-cyber-front-in-the-ukrainian-crisis/)

tactical advantage: to hamper the use of information-gathering drones by the Organization for Security and Co-operation in Europe, the diplomatic forum that joins the West and the former Soviet Union.[16]

But Russia's work in this area is even broader than that. In October 2015, Washington detected Russian intelligence-gathering vessels and submarines operating near critical undersea data cables.[17] About the same time, U.S. officials reported that a Russian satellite had veered close to an Intelsat satellite that enables Western cyber operations, a worrying maneuver given that Moscow has the capability to knock out or commandeer targeted satellites.[18]

Russia has also broadened cyber operations to include information warfare.[19] Russia divides such warfare into two areas: information-technical, which aligns with the West's definition of electronic warfare and cyber warfare, and information-psychological, which resembles the Western concept of strategic communications and psychological operations.[20]

This distinction is important because of the prominent role of Russia's information warfare efforts. Led by the Kremlin, the Russian military and intelligence agencies conduct operations in the country's own information sphere – its media and internet space – and outside its borders.[21] The difference from the routine politicking of nations is in the molding of an alternate reality – advanced by the most senior levels of Russian leadership, including Putin – that conflicts fundamentally with facts as understood by the West.[22]

A first sign of this new era of hybrid war came in a five-year string of hacking attacks against the United States from 1998 to 2003 known as "Moonlight Maze." While many details remain undiscovered, hackers traced to Russia stole thousands of U.S. military documents containing sensitive information, including encryption technologies.[23]

Subsequent cyberattacks in Estonia in 2007, Georgia in 2008, and currently Ukraine suggest that Russia is further honing its cyber capabilities. In Estonia, suspected Russian hackers were deployed in a dispute over the relocation of a World War II monument from central Tallinn to the Defense Forces cemetery two miles away. The hackers, in some cases using Kremlin IP addresses, launched crippling distributed denial of service attacks, taking down local government websites, the country's Internet infrastructure, and paralyzing its financial industry.[24]

16. Paul McLeary, "Russia's Winning the Electronic War," *Foreign Policy*, October 21, 2015. (http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/)
17. David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times*, October 25, 2015. (http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html); Michael Pizzi, "Could Russia really cut the Internet?" *Al Jazeera America*, October 26, 2015. (http://america.aljazeera.com/articles/2015/10/26/could-russia-really-cut-the-internet.html)
18. Mike Gruss, "Russian Satellite Maneuvers, Silence Worry Intelsat," *SpaceNews*, October 9, 2015. (http://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/); Laurence Peter, "Russia shrugs off US anxiety over military satellite," *BBC News* (UK), October 20, 2015. (http://www.bbc.com/news/world-europe-34581089); Sam Jones, "Satellite wars," *Financial Times* (UK), November 20, 2015. (http://www.ft.com/cms/s/2/637bf054-8e34-11e5-8be4-3506bf20cc2b.html)
19. Kier Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," *5th International Conference on Cyber Conflict*, 2013, pages 1-17. (https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf)
20. Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies*, 2014.
21. Jolanta Darczewska, "The Devil Is in the Details: Information Warfare in the Light of Russia's Military Doctrine," *Ośrodek Studiów Wschodnich* (Poland), May 2015. (http://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf)
22. Simon Shuster, "Inside Putin's On-Air Machine," *Time*, March 5, 2015. (http://time.com/rt-putin/)
23. Adam Elkus, "Moonlight Maze," *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Eds. Jason Healey and Karl Grindal, (Cyber Conflict Studies Association, 2013).
24. Andreas Schmidt, "The Estonian Cyberattacks," *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Eds. Jason Healey and Karl Grindal, (Cyber Conflict Studies Association, 2013), pages 174-93.

The 2008 cyberattacks in Georgia, coinciding with the Russian-Georgian war, may be the first time that Moscow tightly integrated cyber tools into military planning and operations. These attacks, conducted by proxy actors (self-declared "patriotic" Russian hackers and the nationalist youth group Nashi), sought to inflict greater harm and confusion than it managed in Estonia by adding infrastructure system break-ins and Internet traffic diversions and blocking.[25]

Three days before the launch of the 2008 Georgian war, an explosion in Turkey ruptured the Baku-Tbilisi-Ceyhan oil pipeline, putting it out of operation for almost three weeks. According to Western intelligence agencies, Russia triggered the explosion through a cyberattack that penetrated the pipeline's control systems.[26] And in December 2015, experts implicated a Russian hacker group in power blackouts in western Ukraine, the first publicly recorded electric outage blamed on a cyberattack.[27]

It is clear, then, that the DNC hack did not occur in a vacuum. Advanced Persistent Threat 28, or APT28, is one of two groups thought to have conducted the DNC hack. In an ultimately unsuccessful operation in April 2015, APT28 was caught spying on Western discussions of the sanctions regime against Moscow.[28] A few months earlier, the group penetrated and took over TV5, a French television channel, and masked it as a jihadist cyberattack. The attack took the channel off-air for hours, during which the perpetrators posted ISIS-related updates on its social media accounts.[29]

The DNC hack, however, would be by far APT28's most ambitious operation. The sophistication of the string of attacks in Washington, and the palpable danger to the bedrock of the U.S. political system, calls for the White House and Congress to bolster both policy and cyber defenses.

Conclusions and Recommendations

1. **Tighten cyber- and information-security.** The U.S. and EU should enhance a common defense against cyber-intrusion and information warfare, including military and civilian exercises and public-private partnerships. Western forces deployed to the Baltic republics and Eastern Europe should be equipped and trained to continue to operate when lacking control of the information space or the electro-magnetic spectrum.

2. **Prepare sanctions.** If the FBI determines that Russia was responsible for the DNC break-in and identifies those responsible, President Obama should impose sanctions both against officials directly involved and others who influence policy.

25. Andreas Hagen, "The RussoGeorgian War 2008," *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Eds. Jason Healey and Karl Grindal, (Cyber Conflict Studies Association, 2013), pages 194-204.
26. Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era," *Bloomberg*, December 10, 2014. (http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar)
27. Pavel Polityuk, "Ukraine to probe suspected Russian cyber attack on grid," *Reuters*, December 31, 2015. (http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231); Robert M. Lee, "Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered," *SANS Industrial Control Systems Security Blog*, January 1, 2016. (https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered); John Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks," *iSIGHT Partners*, January 7, 2016. (http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/)
28. Alan Katz and Michael Riley, "Russian Hackers Use ZeroDays to Try to Get Sanctions Data," *Bloomberg*, April 18, 2015. (http://www.bloomberg.com/news/articles/2015-04-18/russian-hackers-use-zero-days-in-attempt-to-get-sanctions-data)
29. Aurelien Breeden and Alissa J. Rubin, "French Broadcaster TV5 Monde Recovers After Hacking," *The New York Times*, April 9, 2015. (http://www.nytimes.com/2015/04/10/world/europe/french-broadcaster-tv5-monde-recovers-after-hacking.html); Cale Guthrie Weissman, "France: Russian hackers posed as ISIS to hack a French TV broadcaster," *Business Insider*, June 11, 2015. (http://www.businessinsider.com/new-discovery-indicates-that-russian-hackers-apt28-are-behind-the-tv5-monde-hack-2015-6)

3. **Use the UN as a forum.** The president should elevate the issue of cyber-intrusions at the UN General Assembly next month in New York. He should prioritize the elevation of deterrence against cyberattacks through an alliance of likeminded nations.

4. **Prepare cyber counter-measures.** Should Russia or any other foreign actor be found to be using cyberattacks to disrupt sensitive U.S. government or private systems on a chronic basis, the administration should be prepared to deploy counter-measures including a counter cyberattack.

Under Putin, cyberspace is central to a permanent war footing that advances a long-term objective of re-establishing Soviet-era geo-strategic parity with the United States and its European allies. Moscow's apparent collaboration in the WikiLeaks release has naturally triggered fears that Putin is now testing the U.S. response to a more aggressive Russian offensive. The attack suggests that Putin's Russia will be one of the primary challenges confronted by the next president, one that now extends to U.S. soil.