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, and invaded and annexed territory belonging to Russia's neighbors. 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. 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. 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. Before that, however, Russia broke into President Barack Obama's unclassified email, along with the email servers of the State Department and the Joint Chiefs of Staff. According to CrowdStrike, Russia hacked the Clinton Foundation and several think tanks associated with


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. 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.

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.

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.” 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.

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. 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.”

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. At the same time, Moscow carried out similar jamming in Eastern Ukraine. 


tactical advantage: to hamper the use of information-gathering drones by the Organization for Security and Cooperation in Europe, the diplomatic forum that joins the West and the former Soviet Union.\(^\text{16}\)

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.\(^\text{17}\) 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.\(^\text{18}\)

Russia has also broadened cyber operations to include information warfare.\(^\text{19}\) 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.\(^\text{20}\)

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.\(^\text{21}\) 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.\(^\text{22}\)

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.\(^\text{23}\)

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.\(^\text{24}\)


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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.


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.

---

The Foundation for Defense of Democracies’ Center on Sanctions and Illicit Finance (CSIF) provides policy and subject matter expertise in areas of illicit finance, financial power, and economic pressure to the global policy community. CSIF seeks to illuminate the critical intersection between the full range of illicit finance and national security, including money laundering, terrorist financing, sanctions evasion, proliferation financing, cyber crime and economic espionage, and corruption and kleptocracy. For more information on CSIF’s work, please visit www.defenddemocracy.org/csif.