Update on Russian interference in 2016 U.S. Presidential election

According to the U.S intelligence community, Russian agents attempted to interfere with the 2016 presidential election in the United States. In October 2016, the U.S. government announced that it was “confident” that Russia was behind a computer hack of the Democratic National Committee (DNC) and other political organizations of the Democratic Party. The hackers gained access to tens of thousands of emails, which were forwarded to the Wikileaks website, and then published in the run up to the election.

On December 29, 2016, the White House declared that Russia’s “cyber activities were intended to influence the election, erode faith in U.S democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government. These actions are unacceptable and will not be tolerated.” On that date, the President amended an Executive Order to authorize sanctions on those who “[t]amper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.” Under this authority, the President imposed sanctions on two Russian intelligence services (the GRU and the FSB); four individual GRU officers; and three companies alleged to have provided material support to the GRU’s cyber operations. On January 6, 2017, the Office of the Director of National Intelligence released an unclassified report detailing the Russian campaign to influence the election, which is available here.

Investigations into Russian involvement in the presidential campaign are ongoing; nonetheless, a number of international law issues arise from what is already known about these activities.

1) Attribution: Who hacked the DNC?

Sophisticated cybercriminals and hackers typically use a variety of technical means to avoid detection. As a result, it can be difficult to identify the individuals behind breaches of computer security. Moreover, even when intelligence agencies believe that they have strong evidence on attribution, they may decline to publically release this information, on the grounds that doing so may reveal intelligence capabilities and compromise future operations. For example, when the United States government publically blamed North Korea for a 2014 hack into the computer systems at Sony Pictures, it did not release the evidence that led the government to that conclusion.

One aspect of the determination of attribution is factual: what actor or actors executed the hacks? For example, an entity known as “Guccifer 2.0” claimed responsibility for the DNC hacks, but U.S. intelligence officials have identified “Cozy Bear” and “Fancy Bear,” two hacking entities thought to be associated with Russian intelligence agencies, as the responsible parties.

As a presidential candidate, Donald Trump highlighted the difficulties associated with asserting attribution claims. In a presidential debate, he stated with respect to the DNC hacks: “I mean, it could be Russia, but it could also be China. It could also be lots of
other people. It could be somebody sitting on their bed that weighs 400 pounds, OK? You don’t know who broke in to [the] DNC.”

In the murky world of cyberattacks, what level of proof should be required before a state attributes hacking activities to another state? Should a state be required to make its evidence public when it attributes an attack to another actor? Before it takes actions against the alleged attacker?

A second dimension of attribution is legal: under what conditions is a state responsible for the acts of hackers? In October 2016, the Department of Homeland Security and Director of National Intelligence released a joint statement declaring that the thefts of DNC emails originated from Russian servers, but that they were not able to connect these servers to the Russian government.

Recall that, as discussed in Chapter 14, the ILC Articles on Responsibility of States for Intentionally Wrongful Acts provide that “[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group is in fact acting on the instructions of, or under the direction or control of, that State in carrying out its orders.” Art. 8 (see textbook pages 830-31).

Are tests for attribution developed in other contexts, such as that found in the ILC Articles on Responsibility, well suited for application to activities in cyberspace? What level of control must a state exercise before computer attacks by non-state actors can be attributed to the state?

2) Breach of the norm of non-intervention?

In its Nicaragua v United States opinion, excerpted in Chapter 13, the ICJ stated that “the principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law.” The Court also said that an intervention is “prohibited” when it “bear[s] on matters in which each State is permitted, by the principle of State sovereignty to decide freely.” It continued: “Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention.”

In light of the ICJ’s analysis, how should “coercion” be understood in the context of cyber-intelligence operations and cyberhacks? Should international law deem any effort to interfere with foreign elections an impermissible form of intervention into the affairs of another state? If not, how would you distinguish permissible from impermissible forms of interference?
3) What law applies in cyberspace?

A larger, background question posed by this fact pattern is how, if at all, does international law apply in cyberspace? A UN Group of Governmental Experts has explored this question, and in a 2013 report concluded that “international law and in particular the UN Charter, is applicable” to activities in cyberspace. In a 2015 report, the Group declared that “States must observe, among other principles of international law, State sovereignty, sovereign equality … and non-intervention in the internal affairs of other States.” In 2013, a different group of experts issued the Tallinn Manual, which addresses the law applicable to cyber warfare, and which concludes that cyber operations that constitute a threat or use of force against the territorial integrity or political independence of any State are unlawful, and that cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.

In February 2017, an updated and considerably expanded Tallinn Manual 2.0 was released. It argues that pre-cyber era international law applies to cyber operations, both conducted by and directed against states. The Tallinn Manual 2.0 analyzes not only cyber operations that violate the prohibition on the use of force, but also the more common cyber incidents that states encounter with increasing frequency that fall below the thresholds of use of force or armed attack.

What logic supports the application of preexisting international legal norms in the domain of cyberspace? Or, do the unique features of networked technologies and cyberspace suggest that traditional norms need to be adapted, or new norms developed? If new norms are needed, should these be developed in a treaty negotiating process? Given rapid technological changes, are the more decentralized and behavioral processes of customary international lawmaking more appropriate? Or do rapidly changing technologies make soft law options more attractive?

For more on these issues, see Duncan Hollis, Russia and the DNC Hack: What Future for a Duty of Non-Intervention, at opinionjuris.org; Steven J. Barela, Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion, at justsecurity.org.