The DNC Hack Was Not an Act of War

What we call it under international law should influence our response

By Daniel Garrie / Law & Forensics LLC & Joey Johnson / Premise Health

For weeks and months, countless news cycles have been spent discussing Russia's alleged hacking of the Democratic National Committee (DNC); the Obama administration's decision to take steps against Russia in response to that alleged hacking; and, most recently, Michael Flynn's resignation from his position as national security adviser. The debate surrounding the DNC hack, interestingly, has not fallen along party lines. It has ranged widely in content – from President Trump's outright denial of Russian involvement to John McCain's claim that Russian involvement constitutes an act of war.

While much of the rhetoric has been strong, we have seen no real discussion of legal merit. Determining the legal merit of these positions, however, is crucial in such a high-stakes situation. So, we have carefully and dispassionately reviewed the categories of international violations of sovereignty, and, on the basis of the available evidence, we have come to several conclusions, First, even assuming that all the accusations against Russia are true, its actions are more akin to an interference with a nation state's internal affairs than an "act of war." This means that neither group, whether the deniers or the war hawks, is correct. Therefore, we believe that the appropriate course of action in responding to the alleged hack must, under legal principles governing such interference, occupy the middle ground.

The Background

Many intelligence agencies have come out in recent weeks and attributed the hack of the DNC to Russia. Yet, the question of attribution still plagues the discussion, with President Trump famously remarking that it could have been a state actor or a 400-pound hacker sitting on his bed in New Jersey. While his comments highlight a critical and fundamental issue in cyber warfare, we will presume, for this discussion, that the cyberattack resulted from a state-actor from Russia deliberately interfering with the United States' electoral process.

If attribution is resolved, we now turn to whether Russia's actions rise to the level of an act of war. The question for this analysis is whether the action crossed the threshold of "use of force" under the UN Charter Article 2(4), which provides that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

> ***While much of the rhetoric has been strong, we have seen no real discussion of legal merit.***

Does a cyberattack qualify? Obviously the UN Charter did not address that issue. Here's a quotation from one document that did: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force." This definition comes from the Tallinn Manual on the International Law Applicable to Cyber Warfare, a military manual published by an international group of experts working with the NATO Cooperative Cyber Defense Center of Excellence. It has been widely accepted by the community of nations. The Tallinn Manual goes on to say that "cyber psychological operations intended solely to undermine confidence in a government […] does not qualify as a use of force," and that "whatever force may be, it is not mere political coercion." It is relatively clear that, by these legal definitions, whatever actions the Russian government is accused of taking do not constitute a "use of force" sufficient to be deemed an act of war permitting the United States to respond militarily.

If these actions are not an act of war, what are they? International law prohibits the intervention by one state into the domestic affairs of another. Russia's actions in hacking the DNC, and releasing the hacked information, purportedly to sway the U.S. presidential election, are the very definition of a state intervening in the domestic affairs of another. In international governance associated with state-based hacking, the question is whether the actual direct compromise of the DNC systems and data is perceived as a transgression distinct from the later act of publicly releasing that information. Espionage is defined under a certain context, but may include theft of material information. For the spying nation to use that material internally represents a different scenario than if it publicizes the material to the world.

While not an act of war, it is a wrongful act, sufficient to permit countermeasures. Under Rule 9, the Tallinn Manual says: "A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State." However, ambiguity remains in determining what actually represents "proportionate countermeasures." First of all, the challenge of attribution is complex, as a nation-state may indirectly sponsor aggressive cyber activities through a non-state-affiliated entity. In a scenario where that entity is operating from another nation-state, the ramifications of actions against that separate state introduce significant complexities. Furthermore, the ecosystem of secretive encrypted networks, such as Tor, that provide user anonymity and the prevalence of equally protective alternative electronic currencies like Bitcoin, add additional challenges to proving attribution. Nonetheless, it is critical to overcome this challenge to ensure that "proportionate countermeasures" are focused on the right target, and only the right target.

Even in a scenario where the challenge of defensible attribution can be put aside, and we can assume that the attribution is correct, the notion of "proportionate" also introduces legalistic complexities. Countermeasures are not necessarily an eye for an eye. China, for example, has no equivalent open election to hack. So, what countermeasures would be deemed a response versus an initial unrelated campaign? This remains an area that requires more clarification under international cyberlaw.

Nonetheless, in this scenario, with a better understanding of the existing legal definitions of the actions that the Russian government undertook, we can now better understand why both the deniers and the war hawks are not only incorrect, but dangerously so. Regarding the war hawks, encouraging the United States to treat Russia's actions as an act of cyberwar, instead of an intervention into domestic affairs, pushes the United States to respond and escalate (a course only justified if the Russian conduct was an act of war). Treating this incident as an act of war risks setting off a large-scale conflict crossing all domains of warfare, including kinetic warfare.

The deniers err by not giving proper emphasis to state sovereignty – admittedly, an easier thing to do when the interference with state sovereignty occurs by way of cyberintrusions rather than tanks and planes. Paired with the difficulty of attribution, there is an impulse to permit, or strategically overlook, violations of sovereignty in the cyber realm that do not rise to the level of an act of war. However, much like broken-windows policing, demonstrating a willingness to respond proportionately to all violations of state sovereignty deters future violations of state sovereignty – future violations that may well increase in severity and scope.

The election showcased the strength and dangers of cyber operations. A nation-state need not crash a power grid or hack a dam to dramatically affect the affairs of another sovereign state. There are a multitude of ways to do so, and it behooves us to develop countermeasures appropriate for every level of violation of sovereignty in the cyber realm. Neither jingoistic overescalation nor willful ignorance and denial constitutes an effective long-term strategy. Rather, measured and proportionate responses, founded in the rule of law, is the soundest plan. Quantifying what justifiably constitutes "measured and proportionate" is the challenge that remains in front of us.

Daniel Garrie *is an arbitrator, forensic neutral and technical special master at JAMS, available in Los Angeles, New York and Seattle. He is executive managing partner of Law & Forensics LLC, and head of its computer forensics and cybersecurity practice groups, with locations in the United States, India and Brazil. He is also a Cybersecurity Partner at Zeichner Ellman & Krause LLP. He can be reached at Daniel@lawandforensics.com.*

Joey Johnson *is chief information security officer at Premise Health, a provider of employer-sponsor health and wellness centers for employees. He is responsible for leading all organizational efforts related to security operations and engineering, information technology and security compliance. He can be reached at Joey.Johnson@PremiseHealth.com.*