# Cyber Strategy & Policy:
# International Law Dimensions

## Testimony Before the Senate Armed Services Committee

**Matthew C. Waxman**
Liviu Librescu Professor of Law, Columbia Law School
Co-Chair, Columbia Data Science Institute Cybersecurity Center

**March 2, 2017**

Chairman McCain, Ranking Member Reed, members of the committee, and staff. I appreciate the opportunity to address this critical topic.

In discussing cyber policy and deterrence, I have been asked specifically to address some of the international law questions most relevant to cyber threats and U.S. strategy. These include whether and when a cyber-attack amounts to an "act of war," or, more precisely, an "armed attack" triggering a right of self-defense. I would also like to raise the issue of how the international legal principle of "sovereignty" could apply to cyber activities, including to the United States' own cyber-operations.

These are important questions because they affect how the United States may defend itself against cyber-attacks and what kinds of cyber-actions the United States may itself take. They are difficult questions because they involve international rules, developed in some cases over centuries, to deal with new and rapidly changing technologies and forms of warfare.

To state up-front my main points: International law in this area is not settled. There is, however, ample room within existing international law to support a strong cyber strategy, including a powerful deterrent. The answers to many international law questions discussed below depend on specific, case-by-case facts, and are likely to be highly contested for a long time to come. This means that the United States should continue to exercise leadership in advancing interpretations that support its strategic interests, including its own operational needs, bearing in mind that we also seek rules that will effectively constrain the behaviors of others.[1]

---

[1] This testimony draws heavily on two previous articles: Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law*, Vol. 36 (2011) (available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1403&context=yjil); and Matthew C. Waxman, "Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Law Studies*, Vol. 89 (2013) (available at http://stockton.usnwc.edu/ils/vol89/iss1/19/).

Before turning to some specific questions, let me say a few words about why international law matters here, and why it is important that the U.S. government continues to refine, explain and promote diplomatically its legal positions on these issues. Besides American commitment to rule of law and treaty obligations, international law is relevant to U.S. cyber strategy in several ways. Established rules and obligations help influence opinions and shape reactions among audiences abroad, and they therefore raise or lower the costs of actions. They may be useful in setting, communicating and reinforcing "red lines," as well as for preserving international stability, especially during crises. Agreement on them internally within the government can speed decision-making. And agreement on them with allies can provide a basis for cooperation and joint action.

In approaching these legal questions, the U.S. government also must think through what legal rules or interpretations it seeks to defend itself as well as how those legal rules might limit its authority to carry out its own cyber-operations. And, of course, the same rules and interpretations advanced by the United States may be used by other states to help justify their own actions.

With those objectives in mind, I will turn to some specific international legal questions.

First, it is sometimes asked whether a cyber-attack could amount to an "act of war." More broadly, how are cyber-attacks classified or categorized under international law? When should a cyber-attack be treated legally the same way we would treat a ballistic missile attack, for example, versus an act of espionage, or an act of economic competition? Or should actions carried out in cyberspace be treated altogether differently, with entirely new rules? One reason this matters is that certain broad categories of hostile actions are prohibited under well-established international law. Another reason is that how a hostile action is categorized under international law is relevant to what types and levels of defensive responses are permitted. That is, different legal categories of hostile acts correspond to different legal options for countering them.

The term "act of war" retains political meaning, usually to signify the hostile intent and magnitude of threat posed by an adversary's actions. As a technical legal matter, this term has been replaced by provisions of the United Nations Charter. That central, global treaty created after World War II prohibits the use of "force" by states against each other, and it affirms that states have a right of self-defense against "armed attacks."[2] Historically, those provisions had generally been interpreted to apply to acts of physical violence. Questions arise today, though, as to how these provisions should be interpreted to account for the grave harms that can be inflicted through hacking and malicious code, rather than bombs and bullets.

A more legally precise way to frame the "act of war" question, then, is whether a cyber-attack could violate the UN Charter's prohibitions of force or could amount to an armed attack.[3] Even if

[2] Most international lawyers agree that the right of self-defense includes right to use force in anticipatory self-defense to prevent an imminent attack, and this should be true in cyber as well, though determining the "imminence" of an attack is likely to be especially challenging.

[3] With regard to conventional military force, the United States has in the past taken the position that there is no gap between a use of "force" and an "armed attack." Many international lawyers

a cyber-attack does not rise to those thresholds—take, for example, a hack of government systems that results in the theft of large amounts of sensitive data—the United States would still have a broad menu of options for responding to them. And even cyber-attacks that do not amount to force or armed attack may nevertheless violate other international law rules, some of which I discuss below.[4] However, a cyber-attack that does cross the force or armed attack threshold would trigger legally an even wider set of responsive options, which notably could include military force or cyber-actions that would themselves otherwise constitute prohibited force.

Similar questions arise in interpreting mutual defense treaties, such as the North Atlantic Treaty, to account for cyber-threats. Those commitments include collective responses to "attacks," which historically meant kinetic military attacks but might be invoked in response to attacks carried out in cyberspace.[5]

In recent years the United States government has definitively taken the public position that *some* cyber-attacks, even though carried out through digital means rather than kinetic violence, *could* cross the UN Charter's legal thresholds of "force" or "armed attack."[6] In taking that position, it

---

disagree, however, and treat armed attack as a higher threshold. I have noted in the past that the application of these rules to cyber-attacks may require some rethinking of this issue. Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law*, Vol. 36 (2011), pp. 438-440.

[4] Some cyber-attacks that do not fall within these categories may, for example, still violate other international legal principles (such as the principle of "sovereignty," discussed below); specific provisions of other bodies of international law, such as space law; or a state's domestic law. As a general matter, states may respond to violations of international law that do not constitute an armed attack with "countermeasures." Countermeasures are defensive actions that would otherwise be illegal but are intended to bring a violator into compliance with international law. And even unfriendly actions that are within the bounds of international law, such as spying, may be addressed with "retorsion," or unfriendly but legal acts. Examples of retorsion would be expelling diplomats or economic sanctions in response to a hack. While I do not endorse all of its interpretations, an important survey of many of these issues is contained the recently-published *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017).

[5] NATO has declared collectively that its defense commitments extend to cyberspace, though questions of attack thresholds remain. See NATO, "Cyber Defence" (last updated Feb. 17, 2017), available at http://www.nato.int/cps/en/natohq/topics_78170.htm.

[6] This general position has been declared in a number of statements and official documents, including: Department of Defense Law of War Manual (Dec. 2016 edition); Paper submitted by the United States to the 2014-15 UN Group of Governmental Experts (Oct. 2014); Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012).

That position has developed over time and across presidential administrations, though it remains contested and leaves open many questions. See Jack Goldsmith, "How Cyber Changes the Laws of War," *European Journal of International Law*, vol. 24 (2013), pp. 133-135. In testifying before the Senate Committee considering his 2010 nomination to head the new Pentagon Cyber

has said that these determinations, in a given case, should consider many factors including the nature and magnitude of injury to people and the damage to property. Other relevant factors include the context in which the event occurs, who perpetrated it (or is believed to have perpetrated it) and with what intent, and the specific target or location of the attack. At least for cases of cyber-attacks that directly cause the sort of injury or damage normally caused by, for example, a bomb or missile, the U.S. government has declared it appropriate to treat them legally as one would an act of kinetic violence. In explaining publicly this position, the United States usually provides only quite extreme scenarios, such as inducing a nuclear meltdown or causing aircraft to crash by interfering with control systems.

This approach to applying by analogy well-established international legal rules to new technologies is not the only reasonable interpretation, but it is generally sensible and can accommodate a strong cyber strategy. It is likely better than alternatives such as declaring the UN Charter rules irrelevant to cyber or trying to negotiate new international legal rules from scratch.

However, the U.S. government's approach to date in interpreting the UN Charter for cyber-attacks, at least as explained publicly, may seem unsatisfactory to policymakers and planners. It leaves a lot of gray areas (though even in the more familiar world of physical armed force there are many legal gray areas). It is difficult to draw clear legal lines in advance when the formula calls for weighing many factors. And it leaves open how to treat legally some cyber-attacks that do not directly and immediately cause physical injuries or destruction but that nevertheless cause massive harm—take, for instance, a major outage of banking and financial services—or that weaken our defense capability—such as disrupting the functionality of military early warning systems.

In terms of policy, it may therefore be useful to draw sharper "red lines" than the United States has done to date—though because of ambiguities it would be difficult to use international legal

---

Command, Lieutenant General Keith Alexander explained that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace." He went on to suggest, however, that "[i]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response." Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the Senate Armed Services Committee (Apr. 15, 2010). A 1999 Defense Department *Assessment of International Legal Issues in Information Operations* that, taking account of their consequences, some cyber-attacks could constitute armed attacks giving rise to the right of military self-defense.

boundaries alone as the basis for clear and general line-drawing. The United States has been pushing for, and should push for, certain norms of expected behavior in cyberspace (which may not be formally required), and similarly it should continue to discuss or negotiate with rivals some specific mutual restraints on cyber-attacks on particular types of targets, along with confidence-building measures.

In terms of international law, however, I do not expect that precise answers to these questions about "force" and "armed attack" will, or can, all get worked out quickly. The scenarios for cyber-attacks are very diverse and the processes by which international law develops—much of it through the actions and arguments, counter-actions and counter-arguments of states—are slow.[7]

Although the "act of war" or, more precisely, "armed attack" question usually attracts more attention, I want to raise for your consideration another relevant international law issue: the meaning of state "sovereignty" in the cyber context.[8] The United States cares deeply about preserving its own sovereignty. I would emphasize also, though, that the meaning of that concept in the cyber context—or how the U.S. government interprets the principle of sovereignty as it applies to digital information and infrastructure—could have significant impact on the offensive and defensive operational options available to the United States.[9]

"Sovereignty" is a well-established principle of international law. In general, it protects each state's authority and independence within its own territory (and a closely related concept in

---

[7] As I have previously written:

> [I]ncremental legal development through State practice will be especially difficult to assess because of several features of cyber attacks. Actions and counteractions with respect to cyber attacks will lack the transparency of most other forms of conflict, sometimes for technical reasons but sometimes for political and strategic reasons. It will be difficult to develop consensus understandings even of the fact patterns on which States' legal claims and counterclaims are based, assuming those claims are leveled publicly at all, when so many of the key facts will be contested, secret, or difficult to observe or measure. Furthermore, the likely infrequency of "naked" cases of cyber attacks—outside the context of other threats or ongoing hostilities—means that there will be few opportunities to develop and assess State practice and reactions to them in ways that establish widely applicable precedent.

Matthew C. Waxman, "Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Law Studies*, Vol. 89 (2013), p. 121.

[8] Some of these issues are discussed in Brian J. Egan, Legal Adviser, Department of State, Remarks on International Law and Stability in Cyberspace, Berkeley Law School (Nov. 10, 2016).

[9] Very similar issues arise with respect to the international legal principle of "neutrality" during armed conflicts.

international law is the principle of "non-intervention).[10] But sovereignty is not absolute and its precise meaning is fuzzy—even in physical space, let alone cyberspace. Questions could arise as to whether cyber-activities, including U.S. offensive cyber-actions or defensive cyber-measures, that occur in or transit third-countries without their consent might violate their sovereignty. Because of the global interconnectedness of digital systems, including the fact that much data is stored abroad and constantly moving across territorial borders, the answer to such questions could have far-reaching implications for cyber-operations.

I am mindful, as a policy matter, that we have a strong interest in limiting infiltration and manipulation of our own digital systems. However, it is my view that there is not enough evidence of consistent and general practice among states, or a sense of binding legal obligation among states, to conclude that the principle of sovereignty would prohibit cyber-operations just because, for example, some cyber-activities take place within another state, or even have some effects on its cyber-infrastructure, without consent. It may usually be wise to seek that consent from states that "host" digital systems that might be affected or used in cyber-operations, but I am skeptical of legal interpretations of sovereignty that impose extremely strict requirements to obtain it, especially when the effects are minimal.

This is not the setting to discuss operational issues in detail. I expect, though, that such questions about how sovereignty principles apply to cyber-operations, like questions "force" and "armed attack" thresholds, will remain the focus of intense discussion within the U.S. government and with allies and partners abroad.

* * *

I will conclude by reiterating that existing international law, although not yet settled, is adequate to support a strong cyber-defense strategy, including a powerful deterrent. The answers to many international law questions, such as those I have discussed, depend on specific, case-by-case facts, and are likely to be highly contested for a long time to come. This means that the United States should continue to exercise leadership in advancing interpretations that support its strategic interests, including its own operational needs, bearing in mind that we also seek rules that will effectively constrain the behaviors of others.

[10] For a discussion of these principles and some possible interpretations (among many) for cyber-operations, see the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017), pp. 11-27, 312-325.