Cyber-War and the Law of Armed Conflict

Moderator: Professor Samuel Rascoff, New York University School of Law

Panelists: Professor Harold Koh, Yale Law School
Professor Matthew Waxman, Columbia Law School
Professor Ashley Deeks, University of Virginia Law School
Colonel Gary Brown (Ret.), International Committee of the Red Cross

This panel explored how and whether laws and norms developed based on conventional warfare should apply to cyber-attacks—attacks that may cause substantial, tangible harm but do not resemble a typical act of war like dropping a bomb. Complicating matters further is the difficulty of developing new laws and norms in an area that is inherently secretive: cyber-attackers do not announce who they are and the victims may not want to admit having been vulnerable.

Professor Samuel Rascoff began the discussion by distinguishing cyber-warfare from other conduct in cyberspace. Perhaps the only publicly known instance of cyber-warfare, he said, is the "Stuxnet" worm, which was jointly created by Israel and the United States and which damaged 1,000 centrifuges in an Iranian nuclear facility. By comparison, in 2012, Iran initiated a cyber-attack that allegedly damaged 30,000 computers at the Saudi oil company Aramco but did not directly impact Aramco's physical infrastructure. Somewhere between the Stuxnet attack and the Aramco attack, Professor Rascoff said, likely lies the important distinction between what is and what is not an act of war.

Professor Rascoff suggested framing the conversation by comparing the strategic, policy and legal questions to those that were facing the world on the eve of the Cold War, when the prospect of nuclear war was reshaping power and reshaping the law. This comparison can be seen in three ways.

First, cyber-war raises strategic questions: Who will be using these cyber-weapons, and how will they be used? Will they be used strategically the way that nuclear weapons have been as a way of shaping or reshaping the global balance of power? Will they be used tactically or operationally in conjunction with traditional conventional nuclear weaponry? What would escalation look like in cyberspace? What does deterrence look like in cyberspace?"

Second, cyber-war raises questions about what institutions will be relevant. The United States has taken the lead in this area, as it did during the Cold War. The key institution is the U.S. Cyber Command, which is co-located with the NSA and which operates mainly in cyberspace.

Third, cyber-war raises legal questions: What counts or what ought to count as a use of force within the meaning of the *jus ad bellum* (the law of going to war) in international law for purposes of cyber-warfare? Should it be a test about breaking things and killing people in the world or should it be some other kind of test? When is an act of self-defense justified in connection with cyber-warfare?

Before turning to the panel, Professor Rascoff raised two complicating factors that distinguish cyber-war from nuclear war—secrecy and attribution. Whereas there was a mushroom cloud over Hiroshima and Nagasaki, there is no such equivalent in cyberspace. Stuxnet became public only because the virus accidently migrated outside Iran. And even if the cyber-attack becomes known, it is often unclear who has initiated it.

Professor Rascoff turned the discussion first to Professor Harold Koh, who was most recently the State Department's Legal Adviser and who published a speech about the application of the law of armed conflict to cyberspace.[3] Professor Rascoff asked Professor Koh whether there has been a new norm applying the law of armed conflict to cyberspace, and what challenging issues have arisen.

Professor Koh responded with some of the key themes of his published speech. At the outset, he echoed Professor Rascoff's point that cyber-war is only one of many activities in cyberspace. There can be all manner of cyber-intrusions, such as cyber-espionage, but those intrusions can, in a manner of minutes, turn into an attack. While there is a clear conceptual difference between exploiting a computer network and attacking it, the difference is "virtually meaningless" in practice because countries and companies have to respond to both.

Professor Koh next said that the United States has made clear that cyberspace is not a "law-free" zone and that the laws of war *do* apply to cyber-war. It is self-evident, he said, that causing a hospital to lose electricity and thereby causing people to die is no different from dropping a bomb. The harder questions arise when the physical harm is less manifest.

Other principles of the law of war apply to cyberspace, including the law of conducting a war (*jus in bello*). For example, it is unlawful to attack civilians or respond disproportionately.

[3] A copy of the speech is available at http://www.state.gov/s/l/releases/remarks/197924.htm.

But these principles can be tricky in cyberspace because of the need for swift countermeasures. "Something that looks like a response in self-defense can quickly become something that looks offensive," Professor Koh said.

Further, the line between civilian and military is less clear in cyberspace because there is often "dual use" infrastructure, such as servers. An attack on a server could damage business infrastructure and thus be considered an attack on civilians.

Professor Koh raised a final question of what institutions should govern in cyberspace. One alternative is to do nothing. Another model would be a state-to-state model in which countries negotiate treaties, but the problem with that model is that cyberspace has traditionally had other stakeholders, including private business.

Professor Rascoff then turned the discussion to Colonel Gary Brown, the first Legal Adviser to the U.S. Cyber Command. Professor Rascoff highlighted a dilemma from Professor Koh's remarks: How do we draw a clean distinction between espionage (which is not regulated) and cyber-war (which, it is generally agreed, should be) when, as Professor Koh pointed out, the difference between the two "can be vanishingly hard to tell?"

Colonel Brown conceded that the question raised a dilemma. He underscored the point with the following illustration: "If you cut the wire around a base and walk on to a base it isn't immediately clear whether or not you might be a saboteur or a spy. The problem in cyberspace is you can change from one to the other in milliseconds and engage in very, very significant espionage very rapidly or you could flip the switch and go the other way and destroy the entire system before it has a chance to respond."

Professor Rascoff then turned the discussion to Professor Ashley Deeks, who has published extensively on cyber-warfare and who previously served as Deputy Legal Adviser of the State Department. He asked how she expected law to be made in this area and to comment on the role that secrecy would play in creating law for cyber-attacks.

Professor Deeks began by saying that there is a general consensus that the law of armed conflict can apply to cyber-attacks if, for example, it resulted in the same kind of harm as "kinetic activity." She said it was not even clear Stuxnet would meet that standard.

Professor Deeks added that states are giving consideration to how various other legal norms can be translated into cyberspace, as well. For example, there are norms providing that (a) a state should have the right to control activities within its territory (territorial sovereignty), (b) states should not excessively interfere in another state's economic, social and political activities (non-intervention) and (c) states should not allow conduct within their territory to spill over and harm neighboring states. The content of these norms is heavily debated—"squishy"—and states are trying to figure out how they apply to cyberspace.

As for the future of making law in this area, Professor Deeks said that international law generally comes in two forms: treaties and customary international law. She said it would be hard to imagine formal treaties in these areas because states do not want to reveal what they are doing. She expected the developments to occur primarily through state practice.

Returning to Professor Rascoff's question about secrecy, Professor Deeks said that states are unlikely to say what they have done and why regarding cyber-attacks. Rather, she expects that international norms will form when there are unauthorized leaks, and when governments are forced to defend what they have done, or norms may develop when states forced to defend against cyber-attacks themselves must explain who attacked them and why those attacks merit a response.

The discussion then turned to Professor Matthew Waxman, who like Professor Deeks, has published extensively on these issues. Professor Waxman also held various government positions in the White House, the State Department and the Pentagon earlier in his career. Professor Rascoff asked Professor Waxman about how the issues discussed would manifest themselves in domestic law and before U.S. courts.

Professor Waxman said that the U.S. government's involvement in an attack, or in defense of an attack, could involve seizing or blocking data or communications in ways that raise property, privacy or free speech issues. This could raise questions about what is justiciable and what degree of deference the courts will give to the government. Should it be the same extensive deference given to the government concerning conventional war?

Generally, there is more deference given to the executive in foreign operations, but, Professor Waxman said, the line between domestic and foreign in cyberspace is a "blurry one." The level of deference would also likely depend on how closely the conduct resembles traditional military conduct. The closer the resemblance, the more likely the courts would defer to the executive, Professor Waxman said.