U.S. DEPARTMENT OF STATE

DIPLOMACY IN ACTION

International Law in Cyberspace

Remarks
Harold Hongju Koh
Legal Advisor U.S. Department of State
USCYBERCOM Inter-Agency Legal Conference
Ft. Meade, MD
September 18, 2012

As prepared for delivery

Thank you, Colonel Brown, for your kind invitation to speak here today at this very important conference on "the roles of cyber in national defense." I have been an international lawyer for more than thirty years, a government lawyer practicing international law for more than a decade, and the State Department's Legal Adviser for nearly 3 ½ years. While my daily workload covers many of the bread and butter issues of international law—diplomatic immunity, the law of the sea, international humanitarian law, treaty interpretation—like many of you, I find more and more of my time is spent grappling with the question of how international law applies in cyberspace.

Everyone here knows that cyberspace presents new opportunities and new challenges for the United States in every foreign policy realm, including national defense. But for international lawyers, it also presents cutting-edge issues of international law, which go to a very fundamental question: *how do we apply old laws of war to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?*

Many, many international lawyers here in the U.S. Government and around the world have struggled with this question, so today I'd like to present an overview of how we in the U.S. Government have gone about meeting this challenge. At the outset, let me highlight that the entire endeavor of applying established international law to cyberspace is part of a broader international conversation. We are not alone in thinking about these questions; we are actively engaged with the rest of the international community, both bilaterally and multilaterally, on the subject of applying international law in cyberspace.

With your permission, I'd like to offer a series of questions and answers that illuminate where we are right now – in a place where we've made remarkable headway in a relatively short period of time, but are still finding new questions for each and every one we answer. In fact, the U.S. Government has been regularly sharing these thoughts with our international partners. Most of the points that follow we have not just agreed upon internally, but made diplomatically, in our submissions to the UN Group of Governmental Experts (GGE) that deals with information technology issues.

I. International Law in Cyberspace: What We Know

So let me start with the most fundamental questions:

Question 1: *Do established principles of international law apply to cyberspace?*

Answer 1: **Yes, international law principles do apply in cyberspace.** Everyone here knows how cyberspace opens up a host of novel and extremely difficult legal issues. But on this key question, this answer has been apparent, at least as far as the U.S. Government has been concerned. Significantly, this view has not necessarily been universal in the international community. At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law *do* apply in cyberspace.

Question 2: *Is cyberspace a law-free zone, where anything goes?*

Answer 2: **Emphatically no. Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint.**

Think of it this way. This is not the first time that technology has changed and that international law has been asked to deal with those changes. In particular, because the tools of conflict are constantly evolving, one relevant body of law – international humanitarian law, or the law of armed conflict – affirmatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation. To be sure, new technologies raise new issues and thus, new questions. Many of us in this room have struggled with such questions, and we will continue to do so over many years. But to those who say that established law is not up to the task, we must articulate and build consensus around how it applies and reassess from there whether and what additional understandings are needed. Developing common understandings about how these rules apply in the context of cyberactivities in armed conflict will promote stability in this area.

That consensus-building work brings me to some questions and answers we have offered to our international partners to explain how both the law of *going to war* (*jus ad bellum*) and the laws that apply in conducting war (*jus in bello*) apply to cyberaction:

Question 3: *Do cyber activities ever constitute a use of force?*

Answer 3: Yes. **Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.** In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.* In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.

Question 4: *May a State ever respond to a computer network attack by exercising a right of national self-defense?*

Answer 4: Yes. **A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.** As the United States affirmed in its 2011 International Strategy for Cyberspace, "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."

Question 5: *Do jus in bello rules apply to computer network attacks?*

Answer 5: Yes. **In the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of necessity and proportionality limit uses of force in self-defense and would regulate what may constitute a lawful response under the circumstances.** There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.

Question 6: *Must attacks distinguish between military and nonmilitary objectives?*

Answer 6: Yes. The *jus in bello* principle of distinction applies to computer network attacks undertaken in the context of an armed conflict. The principle of distinction applies to cyber activities that amount to an "attack" – as that term is understood in the law of war – in the context of an armed conflict. As in any form of armed conflict, the principle of distinction requires that the intended effect of the attack must be to harm a legitimate *military* target. We must distinguish military objectives – that is, objects that make an effective contribution to military action and whose destruction would offer a military advantage – from civilian objects, which under international law are generally protected from attack.

Question 7: *Must attacks adhere to the principle of proportionality?*

Answer 7: Yes. **The *jus in bello* principle of proportionality applies to computer network attacks undertaken in the context of an armed conflict.** The principle of proportionality prohibits attacks that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated. Parties to an armed conflict must assess what the expected harm to civilians is likely to be, and weigh the risk of such collateral damage against the importance of the expected military advantage to be gained. In the cyber context, this rule requires parties to a conflict to assess: (1) the effects of cyber weapons on both military and civilian infrastructure and users, including shared physical infrastructure (such as a dam or a power grid) that would affect civilians; (2) the potential physical damage that a cyber attack may cause, such as death or injury that may result from effects on critical infrastructure; and (3) the potential effects of a cyber attack on civilian objects that are *not* military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are military objectives.

Question 8: *How should States assess their cyber weapons?*

Answer 8: **States should undertake a legal review of weapons, including those that employ a cyber capability.** Such a review should entail an analysis, for example, of whether a particular capability would be *inherently indiscriminate, i.e.*, that it could not be used consistent with the principles of distinction and proportionality. The U.S. Government undertakes at least two stages of legal review of the use of weapons in the context of armed conflict – first, an evaluation of new weapons to determine whether their use would be *per se* prohibited by the law of war; and second, specific operations employing weapons are always reviewed to ensure that each particular operation is also compliant with the law of war.

Question 9: *In this analysis, what role does State sovereignty play?*

Answer 9: **States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict.** The physical infrastructure that supports the internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered.

Question 10: *Are States responsible when cyber acts are undertaken through proxies?*

Answer 10: Yes. **States are legally responsible for activities undertaken through "proxy actors," who act on the State's instructions or under its direction or control.** The ability to mask one's identity and geography in cyberspace and the resulting difficulties of timely, high-confidence attribution can create significant challenges for States in identifying, evaluating, and accurately responding to threats. But putting attribution problems aside for a moment, established international law does address the question of proxy actors. States are legally responsible for activities undertaken through putatively private actors, who act on the State's instructions or under its direction or control. If a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it. These rules are designed to ensure that States cannot hide behind putatively private actors to engage in conduct that is internationally wrongful.

II. International Law in Cyberspace: Challenges and Uncertainties

These ten answers should give you a sense of how far we have come in doing what any good international lawyer does: applying established law to new facts, and explaining our positions to other interested lawyers. At the same time, there are obviously many more issues where the questions remain under discussion. Let me identify three particularly difficult questions that I don't intend to answer here today. Instead, my hope is to shed some light on some of the cutting-edge legal issues that we'll all be facing together over the next few years:

Unresolved Question 1: **How can a use of force regime take into account all of the novel kinds of *effects* that States can produce through the click of a button?**

As I said above, the United States has affirmed that established *jus ad bellum* rules do apply to uses of force in cyberspace. I have also noted some clear-cut cases where the physical effects of a hostile cyber action would be comparable to what a kinetic action could achieve: for example, a bomb might break a dam and flood a civilian population, but insertion of a line of malicious code from a distant computer might just as easily achieve that same result. As you all know, however, there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by "force." At the same time, the difficulty of reaching a definitive legal conclusion or consensus among States on when and under what circumstances a hostile cyber action would constitute an armed attack does not automatically suggest that we need an entirely new legal framework specific to cyberspace. Outside of the cyber-context, such ambiguities and differences of view have long existed among States.

To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response – such responses must still be *necessary* and of course *proportionate*. We recognize, on the other hand, that some other countries and commentators have drawn a distinction between the "use of force" and an "armed attack," and view "armed attack" – triggering the right to self-defense – as a subset of uses of force, which passes a higher threshold of gravity. My point here is not to rehash old debates, but to illustrate that States have long had to sort through complicated *jus ad bellum* questions. In this respect, the existence of complicated cyber questions relating to *jus ad bellum* is not in itself a new development; it is just applying old questions to the latest developments in technology.

Unresolved Question 2: **What do we do about "*dual-use* infrastructure" in cyberspace?**

As you all know, information and communications infrastructure is often shared between State militaries and private, civilian communities. The law of war requires that civilian infrastructure not be used to seek to immunize military objectives from attack, including in the cyber realm. But how, exactly, are the *jus in bello* rules to be implemented in cyberspace? Parties to an armed conflict will need to assess the potential effects of a cyber attack on computers that are *not* military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are valid military objectives. Parties will also need to consider the harm to the civilian uses of such infrastructure in performing the necessary proportionality review. Any number of factual scenarios could arise, however, which will require a careful, fact-intensive legal analysis in each situation.

Unresolved Question 3: **How do we address the problem of *attribution* in cyberspace?**

As I mentioned earlier, cyberspace significantly increases an actor's ability to engage in attacks with "plausible deniability," by acting through proxies. I noted that legal tools exist to ensure that States are held accountable for those acts. What I want to highlight here is that many of these challenges – in particular, those concerning attribution – are as much questions of a technical and policy nature rather than exclusively or even predominantly questions of law. Cyberspace remains a new and dynamic operating environment, and we cannot expect that all answers to the new and confounding questions we face will be *legal* ones.

These questions about effects, dual use, and attribution are difficult legal and policy questions that existed long before the development of cyber tools, and that will continue to be a topic of discussion among our allies and partners as cyber tools develop. Of course, there remain many other difficult and important questions about the application of international law to activities in cyberspace – for example, about the implications of sovereignty and neutrality law, enforcement mechanisms, and the obligations of States concerning "hacktivists" operating from within their territory. While these are not questions that I can address in this brief speech, they are critically important questions on which international lawyers will focus intensely in the years to come.

And just as cyberspace presents challenging new issues for lawyers, it presents challenging new technical and policy issues. Not all of the issues I've mentioned are susceptible to clear legal answers derived from existing precedents – in many cases, quite the contrary. Answering these tough questions within the framework of existing law, consistent with our values and accounting for the legitimate needs of national security, will require a constant dialogue between lawyers, operators, and policymakers. All that we as lawyers can do is to apply in the cyber context the same rigorous approach to these hard questions that arise in the future, as we apply every day to what might be considered more traditional forms of conflict.

III. The Role of International Law in a "Smart Power" Approach to Cyberspace

This, in a nutshell, is where we are with regard to cyberconflict: We have begun work to build consensus on a number of answers, but questions continue to arise that must be answered in the months and years ahead. Beyond these questions and answers and unresolved questions, though, lies a much bigger picture, one that we are very focused on at the State Department. Which brings me to my final two questions:

Final Question 1: *Is international humanitarian law the only body of international law that applies in cyberspace?*

Final Answer 1: **No. As important as international humanitarian law is, it is *not* the only international law that applies in cyberspace.**

Obviously, cyberspace has become pervasive in our lives, not just in the national defense arena, but also through social media, publishing and broadcasting, expressions of human rights, and expansion of international commerce, both through online markets and online commercial techniques. Many other bodies of international and national law address those activities, and how those different bodies of law overlap and interact with the laws of cyber conflict is something we will all have to work out over time.

Take human rights. At the same time that cyber activity can pose a threat, we all understand that cyber-communication is increasingly becoming a dominant mode of expression in the 21st century. More and more people express their views not by speaking on a soap box at Speakers' Corner, but by blogging, tweeting, commenting, or posting videos and commentaries. The 1948 Universal Declaration of Human Rights (UDHR) – adopted more than 70 years ago – was remarkably forward-looking in anticipating these trends. It says: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers*." (emphasis added) In short, all human beings are entitled to certain rights, whether they choose to exercise them in a city square or an internet chat room. This principle is an important part of our global diplomacy, and is encapsulated in the Internet Freedom agenda about which my boss, Secretary Clinton, has spoken so passionately.

You all know of this Administration's efforts not just in the areas of cyber conflict, but also in many other cyber areas: cybersecurity, cybercommerce, fighting child pornography and other forms of cybercrime, stopping intellectual property piracy, as well as promoting free expression and human rights. So the cyberconflict issues with which this group grapples do not constitute the whole of our approach to cyberspace; they are an important part – but only a part – of this Administration's broader "smart power" approach to cyberspace.

What I have outlined today are a series of answers to cyberspace questions that the United States is on the record as supporting. I have also suggested a few of the challenging questions that remain before us, and developments over the next decade will surely produce new questions. But you should not think of these questions and answers as just a box to check before deciding whether a particular proposed operation is lawful or not. Rather, these questions and answers are part of a much broader foreign policy agenda, which transpires in a broader framework of respect for international law.

That leads to my Final Question for this group: *Why should U.S Government lawyers care about international law in cyberspace at all?*

The Answer: **Because compliance with international law *frees* us to do more, and do more legitimately, in cyberspace, in a way that more fully promotes our national interests. Compliance with international law in cyberspace is part and parcel of our broader "smart power" approach to international law as part of U.S. foreign policy.**

It is worth noting two fundamentally different philosophies about international law. One way to think about law, whether domestic or international, is as a straitjacket, a pure constraint. This approach posits that nations have serious, legitimate interests, and legal regimes restrict their ability to carry them out. One consequence of this view is that, since law is just something that constrains, it should be resisted whenever possible. Resisting so-called "extensions" of the law to new areas often seems attractive: because, after all, the old laws weren't built for these new challenges anyway, some say, so we should tackle those challenges without the legal straitjacket, while leaving the old laws behind.

But that is *not* the United States Government's view of the law, domestic or international. We see law not as a straitjacket, but as one great university calls it when it confers its diplomas, a body of "wise restraints that make us free." International law is not purely constraint, it frees us and empowers us to do things we could never do without law's legitimacy. If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we *do* take will earn enhanced legitimacy worldwide for their adherence to the rule of law.

These are not new themes, but I raise them here because of they resonate squarely with the strategy we have been pursuing in cyberspace over the past few years. Of course, the United States has impressive cyber-capabilities; it should be clear from the bulk of my discussion that adherence to established principles of law does not prevent us from using those capabilities to achieve important ends. But we also know that we will be safer, the more that we can rally other States to the view that these established principles *do* impose meaningful constraints, and that there is already an existing set of laws that protect our security in cyberspace. And the more widespread the understanding that cyberspace follows established rules – and that we live by them – the stronger we can be in pushing back against those who would seek to introduce brand new rules that may be contrary to our interests.

That is why, in our diplomacy, we do not whisper about these issues. We talk *openly and bilaterally* with other countries about the application of established international law to cyberspace. We talk about these issues *multilaterally*, at the UN Group of Governmental Experts and at other fora, in promoting this vision of compliance with international law in cyberspace. We talk about them *regionally*, as when we recently co-sponsored an ASEAN Regional Forum event to focus the international community's attention on the problem of proxy actors engaging in unlawful conduct in cyberspace. Preventing proxy attacks on us is an important interest, and as part of our discussions we have outlined the ways that existing international law addresses this problem.

The diplomacy I have described is not limited to the legal issues this group of lawyers is used to facing in the operational context. These issues are interconnected with countless other cyber issues that we face daily in our foreign policy, such as cybersecurity, cyber-commerce, human rights in cyberspace, and public diplomacy through cybertools. In all of these areas, let me repeat again, *compliance with international law in cyberspace is part and parcel of our broader smart power approach to international law as part of U.S. foreign policy*. Compliance with international law – and thinking actively together about how best to promote that compliance – can only free us to do more, and to do more legitimately, in the emerging frontiers of cyberspace, in a way that more fully promotes our U.S. national interests.

Thank you very much.