Remarks to the ICRC Conference, September 11, 2013

- Cyber is a topic that continues to attract much attention. I would like to share with you briefly some U.S. perspectives on the cyber operations and the law of armed conflict (LOAC), also known as international humanitarian law (IHL).

- The relationship between LOAC and cyber is part of a broader question, namely whether existing international law applies to cyber operations at all.

- The United States has made clear its view that existing international law serves as the appropriate framework applicable to online activity in a variety of contexts.

- To be sure, the technology of cyberspace is new. However, certain bodies of international law – including the international law of armed conflict and international human rights law – anticipate technological innovation and contemplate that existing rules will apply to such innovation.

- An important consequence to this recognition is that cyberspace is not a law-free zone. In particular, for the purposes of today’s topic, hostile activities cannot be conducted without rules.

- Thus, for example, the *jus ad bellum* is relevant here. In the U.S. view, under some circumstances, a disruptive activity in cyberspace could constitute an armed attack within the meaning of Article 51 of the UN Charter. And, a State’s inherent national right of self-defense, recognized in that Article of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.

- The fact that it may be difficult to reach a definitive legal conclusion or consensus among States on the circumstances in which a cyber attack would constitute an armed attack does not suggest the need for a new legal framework specific to cyberspace. Such ambiguities are a reflection of the challenges in applying the UN Charter framework that already exist in many contexts.

- Turning now to principles of LOAC, or *jus in bello*: In the context of an armed conflict, the existing rules and principles of the *jus in bello* apply to the use of cyber tools in hostilities, just as they do to other tools.

- For example, 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 *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 civilians and civilian objects, which under international law are generally protected from attack.

- An additional corollary to the principle of distinction is the prohibition on indiscriminate attacks, which may be defined as including attacks that employ a means or method of warfare that by its nature cannot be directed at a specific military objective, or the effects of which cannot be controlled. Weapons that cannot be directed at a specific military objective or whose effects cannot be controlled would be inherently indiscriminate, and per se unlawful under the law of armed conflict. Certain cyber tools could, in light of the interconnected nature of the internet, be inherently indiscriminate in the sense that their effects could not be predicted or controlled; a destructive virus that could spread uncontrollably within civilian internet systems might fall into this category. Attacks using such tools would be prohibited by the law of war.

- In addition to distinction, 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 would require parties to a conflict to assess the effects of cyber weapons on both military and civilian infrastructure and users. In addition to the potential physical damage that a cyber attack may cause, such as death or injury that may result from effects on critical infrastructure, parties should 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 military objectives.

- The jus in bello also requires States that are party to an armed conflict to take all practicable precautions, taking into account military and humanitarian considerations, to avoid and minimize incidental death, injury, and damage to civilians and civilian objects. In the context of hostilities involving cyber tools, parties to the conflict should take precautions to minimize the harm of such cyber activities on civilian infrastructure and users.

- Apart from these two core jus in bello principles, other aspects of the law of armed conflict are also relevant to the use of cyber tools.
• For instance, States should undertake a legal review of weapons, including those that employ a cyber capability. Consistent with the law of armed conflict, the United States undertakes at least two stages of legal review of the use of weapons in the context of armed conflict.
  
  o First, the United States evaluates new weapons and military capabilities for whether their use would *per se* be prohibited by the law of war. In this way, the United States recognizes that weapons and technologies evolve and develop, but that the principles of the law of war continue to apply to new capabilities. Such a review entails 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.
  
  o Second, the United States reviews the deployment of weapons for compliance with the law of war. Specific military operations using weapons are reviewed individually to ensure that each operation would be consistent with the principles of the law of armed conflict discussed above.
  
  o The U.S. Government continues to evaluate the applicability of weapons reviews to cyber capabilities, and reviews cyber capabilities under this framework as appropriate.
  
• Although it is beyond the scope of this presentation to go into details, I want to mention that international humanitarian law is not the only body of international law that may apply to the broad range of online activities, particularly outside of hostilities. For example, principles of sovereignty apply to State conduct in cyberspace. And, when we consider that cyber-communication is increasingly becoming an important mode of expression in the 21st century, we should recall that the rules of international human rights law apply, including in particular the right to freedom of expression, which is well-established internationally in both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Both of these instruments clearly provide that the right to freedom of expression can be exercised through any media and regardless of frontiers.
  
• I noted earlier that there is now broad recognition that existing international law serves as the appropriate framework applicable to online activity. In that connection, I want to mention two recent developments.
  
• First, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security achieved an important result in June of this year. The 15-member expert group reached a consensus affirming that international law, especially the UN Charter, applies in cyberspace. That clear affirmation sends a strong signal: States must act in cyberspace under the established international rules and principles that have
guided their actions in peacetime and during conflict. The final report was issued at the beginning of August, and I hope that you will all have a chance to review it.

Second, earlier this year a group of legal scholars and practitioners published the Tallinn Manual on the International Law Applicable to Cyber Warfare, which sought to set out a series of rules governing such conflicts. This study also endorses the view that existing international law, including the *jus in bello*, applies to activities in cyberspace.

- We have also noticed that there are a number of areas where States and commentators have suggested different views on certain issues. This is not surprising, because there are some complicated questions presented by the application of existing international law to the details of cyberspace.

- In other words, to say that existing international law provides the appropriate legal framework for online activity is not to deny that much work remains to be done in developing a common understanding of how existing legal rules apply to online conduct. For example, States will need to consider the issues raised by infrastructure that is “dual-use” (shared by military and civilian applications). States also need to consider the challenges of attribution of conduct in cyberspace. And, because cyberspace remains a new and dynamic operating environment, we can expect that many of these issues will involve questions of a technical and policy nature, and not just exclusively or perhaps even predominantly questions of law.

- This is not unusual: when new technologies are developed, they often present challenges for the application of existing bodies of law. This has been true for prior developments in the law of armed conflict as well. Moreover, difficult legal questions and differences of opinion also arise in what might be considered the more traditional forms of conflict. Nevertheless, we address those questions through the lens of the existing international law – and, we in the United States are confident, the existing principles of the LOAC will provide that framework for hostilities in cyberspace.