Prepared Testimony and
Statement for the Record of

**Catherine Lotriionte**
**Professor, Georgetown University**

Hearing on

"Cyber War: Definitions, Deterrence, and Foreign Policy"

Before the

House Committee on Foreign Affairs

September 30, 2015

2172 Rayburn House Office Building

Chairman Royce, Ranking Member Engel, Members of the Committee, thank you for the invitation to offer this Statement for the Record on International Law and Cyber Operations.

## Introduction

Even though there has not yet been discrete cyber operations that rise to the level of damage to property and lives equivalent to kinetic attacks, cyber operations are a part of the traditional military operations today, fast becoming a part of modern kinetic warfare. Such cyber operations first appeared overtly in the 2008 armed conflict between Georgia and Russia, were employed during the armed conflicts in Afghanistan and Iraq, figured in operations throughout the armed conflict in Libya and Syria and have played a significant role during the 2014 armed conflict between Russia and Ukraine. The United States has established US Cyber Command to conduct defensive and offensive cyber operations during armed conflicts and other states are following suit by developing cyber capabilities and establishing their force structures to leverage them.

According to a 2013 UN study, 32 states included cyberwarfare in their military planning and organizations. And intelligence reports have noted that more than 140 countries have funded cyber weapon development programs. Cyber operations have already become an integral part of command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) activities in the battlespace and it is inevitable that they will soon play a central role in "attacking" the enemy. The ability to develop these cyber capabilities is also not limited to regular armed forces and states. Non-state actors have also discovered the value of cyber operations as a means of asymmetric warfare.

This emerging reality requires that states examine the question of how to treat cyber operations under international law. There appears no alternative at present but to consider a host of legal propositions in examining the law related to cyber operations and assess whether the laws that we currently have are adequate as cyber operations become ubiquitous. My statement will focus mainly on two areas of international law that are implicated by cyber operations, *jus ad bellum* and *jus in bello*.

## The Applicability of International Law to Cyber Operations Conducted by States

Under international law, "war" is not a meaningful term. The existence of a "war" does not trigger *jus ad bellum* provisions of international law nor is it a necessary trigger for the laws of armed conflict. What is relevant, for purposes of determining the applicability of international law to cyber operations, is to understand the thresholds for "uses of force," "armed attack" and the existence of an "armed conflict" under international law.

Public international law is by nature a dynamic creature that evolves over time through consent of states. The content of this body of law, its interpretation and application develop over time in response to changes in the security environment in which it applies. International law is created by states in two ways: 1) states opting into treaty regimes and 2) state practice that occurs out of a sense of legal obligation (*opinio juris*) or customary international law. For purposes of cyber operations, both *jus ad bellum* and *jus in bello* will have to adapt to the growing threats and new technologies within cyberspace in order to effectively regulate state behavior in this new domain.

Under current international law, cyber operations would amount to internationally wrongful acts if they were inconsistent with established international law. To date, there is only one treaty that explicitly addresses cyber activities: the 2001 Budapest Convention on Cybercrime that requires the state parties to criminalize certain cyber offences in their domestic legislation and to provide mutual assistance in investigations and prosecutions. The lack of treaties and customary international law explicitly addressing cyber operations involving the use of force, however, does not mean that cyber operations can be conducted by states without restrictions.

Cyber operations that amount to a use of force or to acts of hostilities would fall within the provisions of international law that regulate the right of states to use force (*jus ad bellum*) and the conduct of warfare once an armed conflict has broken out (*jus in bello*, also called the laws of armed conflict, LOAC, and international humanitarian law, IHL). In the absence of a specific treaty regulating cyber operations, the question is *whether* and *how* existing treaties and customs that apply to traditional uses of force can be extended to cyber operations. Today, there is a growing international consensus that aspects of international law do apply to the cyber domain but most of the details about how it applies remains in flux.

The key *jus ad bellum* and *jus in bello* treaties are the 1945 Charter of the United Nations, the Hague Conventions of 1899 and 1907, the four 1949 Geneva Conventions on the Protection of Victims of War and their two 1977 Additional Protocols (even though the US is not a party to either). Although these treaties do not mention cyber issues, many states have affirmed the application of existing laws, including the UN Charter and the laws of armed conflict, to cyber operations, usually not distinguishing between treaties and customary international law. Needless to say, states can always conclude less than universal treaties, or even special bi-lateral agreements to expand their obligations under existing international law, *jus ad bellum* and *jus in bello*. Such agreements may be concluded in relation to a particular conflict, or to submit to special protection certain data or critical infrastructure. For example, in the future, there may develop agreement between certain states that cyber operations against essential civilian services, data and critical infrastructure constitute "attacks" under IHL and thereby those states will refrain from conducting such "attacks" and condemn those that conduct them.

In a speech at the US Cyber Command in 2010, the then-legal advisor of the US State Department, Harold Koh, emphasized that international law principles do apply in cyberspace, including but not limited to the *jus ad bellum* and the *jus in bello*. The 2011 White House *International Strategy for Cyberspace* explained that '[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete.' While it is well-settled in the US that the UN Charter and the laws of armed conflict apply to cyber warfare, the challenge is determining exactly *how* it applies and getting international agreement on those issues. As noted in the Department of Defense's *Law of War Manual*, released in June 2015, "[p]recisely how the law of war applies to cyber operations is not well-settled. . ." While there appears to be growing consensus that cyber operations do not exist in a legal or normative vacuum, the law is still in flux and will likely continue to evolve in the future as state practice and *opinio juris* exposes common ground between states as states recognize the shared benefits to agreement on the law.

In 2013, the third Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), established under the auspices of the UN Secretary-General and composed of 15 states, including the US, Russian and China,[1] established agreement on recommendations in its final report on norms, rules, and principles for responsible behaviour of States as well as confidence-building measures and capacity-building. The report affirmed the applicability of international law to cyberspace (explicitly citing the UN Charter); stressing that states must meet their international obligations regarding international wrongful acts attributable to them; states should not use proxies to conduct wrongful acts; and should ensure that their territories are not used by non-state actors for unlawful use of Information and Communications Technologies (ICTs).

In July of this year, the fourth UN GGE, composed of 20 states,[2] finalized its report to the General Assembly. The report highlighted norms for peacetime that states should abide by, including, states should not conduct or knowingly support actions that intentionally damage critical infrastructures of other states; states should assist in requests from other states when their critical infrastructure has been attacked; states should not conduct or support any harmful actions against the information systems of emergency response teams; and states should seek to prevent the proliferation of malicious ICT tools. The report also reiterated the recommendations of the prior UN GGEs, supporting the applicability of international legal obligations in cyberspace, state responsibility for attributable wrongful acts

[1] Additional member states of the 3rd UN GGE were: Argentina, Australia, Belarus, Canada, Egypt, Estonia, France, Germany, India, Indonesia, Japan and the United Kingdom of Great Britain and Northern Ireland.

[2] List of the 20 states in the 4th UN GGE: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Republic of Korea, Russian Federation, Spain, United Kingdom of Great Britain and Northern Ireland, United States.

and the obligation to prevent their state's territory from being used to conduct wrongful acts in cyberspace.

In 2013, a group of twenty international legal experts, who had been convened under the auspices of the NATO Cyber Defence Centre of Excellence in Tallinn, Estonia, published the *Tallinn Manual on the International Law of Cyber Warfare*, which examined the implications under *jus ad bellum* and *jus in bello* of cyber warfare. The Manual includes a set of 95 Rules accompanied by commentaries and while it does not reflect NATO doctrine or the official position of any state or organization, it is a good starting point for further analysis on what international laws are applicable to cyber operations.

**Use of Force (Jus ad Bellum)**

The *jus ad bellum* determines when states may lawfully resort to force in international relations. It is distinction from the *jus in bello* which governs how force may be used once an armed conflict has commenced. In 1945 the UN Charter, in articles 2(4) and 51, redefined previously accepted ideas of *jus ad bellum* and codified the contemporary *jus ad bellum* in its entirety. Article 2(4) states: "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." If a state activity is a use of force within the meaning of Article 2(4), it is unlawful under international law. There are two exceptions in the UN Charter to this general prohibition on the use of force: (1) uses of force authorized by the UN Security Council pursuant to Article 42 of the Charter and (2) individual and collective self-defense in response to an "armed attack" pursuant to Article 51 of the Charter.

Before the advent of cyber operations, states and scholars struggled to define the threshold at which an act becomes a "use of force." Over time, states sought to include a broader range of acts within the meaning of a use of force including acts that would not necessarily be armed but that had aggressive intent. During the 1960s, however, the predominant opinion confined the term to direct uses of or threats to use armed force with aggressive intent justifying defensive military action. It is notable, however, that article 2(4) does not use the word "armed" in reference to force. Today, there is a general understanding that uses of force do not necessarily have to be actions conducted by a state's armed forces to constitute a use of force. It is also accepted that actions involving economic coercion and espionage would fall below the threshold of a use of force. Most international legal scholars today accept that in analyzing actions that may rise to the level of a use of force consideration should be given to the "scale and effects" of the actions rather than focusing solely on whether it involved armed action by a state's forces. In the *Nicaragua* case the International Court of Justice rejected a narrow interpretation of "use of force" that would limit the term to the use of either kinetic force or non-kinetic operations generating comparable effects.

Since the emergence of cyber operations, states and scholars have struggled to define the threshold at which an act in cyberspace would constitute a "use of force" for purposes of Article 2(4) of the Charter. The main challenge in determining whether a cyber operation would be a use of force has been in the application of the rule to cyber operations that, on the one hand, produce severe non-physical consequences but, on the other, do not use destructive or injurious force. Given the lack of a definitive criteria for characterizing an act, in general, as a use of force under international law, it is not surprising that there would be challenges with characterizing cyber operations as uses of force.

Accepting the reasoning of the *Nicaragua* case, the Tallinn Manual adopted an approach concentrating on an act's "scale and effects." (Rule 11 of the Tallinn Manual). This is the same approach articulated in the armed attack context in the *Nicaragua* case. Notice was also taken in the Manual of the discussions at the 1945 UN Charter drafting conference during which economic coercion was regarded by states as not constituting a use of force. Relying on the *Nicaragua* judgment, the Tallinn Manual concluded that non-destructive cyber operations may sometimes amount to a use of force. For example, according to the Manual, while merely funding a hactivist group that is conducting cyber operations, as part of an insurgency, would not qualify as a use of force, arming and training an organized armed group to carry out cyber operations against another state would.

Article 51 of the UN Charter addresses when states may use force in self-defense in response to cyber operations that constitute armed attacks. In line with the *Nicaragua* Court that drew a distinction between uses of forces and armed attacks, the Tallinn Manual concluded that the term "armed attack" differs from "use of force." Only the most grave "uses of force" through cyber operations, the Tallinn Manual experts held, would amount to an "armed attack" triggering the right of a state to use a forcible self-defense measure.[3] The experts agreed that any cyber operation that injures or kills persons or damages or destroys property amounts to an armed attack. The required degree of damage or injury, however, remains the subject of much disagreement. Furthermore, in applying traditional customary principles to cyber operations, any response in self-defense against cyber operations or kinetic attacks amounting to an armed attack, must meet the requirements of necessity, proportionality and immediacy.

Both Harold Koh in his speech and DoD's Law of War Manual apply this traditional "scale and effects" test to the analysis of what would be a use of force or armed attack in cyberspace. According to both, if the physical damage or results of cyber operations were the same as kinetic acts of dropping bombs or firing a missile then the right of self-defense is triggered and traditional laws of war principles of humanity, suffering, injury or destruction unnecessary to accomplish a legitimate

[3] Since the *Nicaragua* decision, the US had rejected the Court's holding that there is a gap between the thresholds for uses of force and armed attacks. In his 2010 speech, Harold Koh reiterated this US position as it applies to cyber operations.

military purpose must be avoided in cyber operations. While the 2015 UN GGE report mentions the language of Article 2(4), it does not provide any detail about possible thresholds and the Russians have indicated that there was disagreement among the member states as to whether Article 51 even applies to cyber operations.

So, while there have been attempts at gaining agreement among states related to how *jus ad bellum* is implicated in cyber operations, uncertainty remains as to where the thresholds for uses of force and armed attacks lie. For example, it remains unclear whether a cyber operation that does not result in physical damage or injury can nevertheless amount to an armed attack, for purposes of Article 51, when it generates severe nondestructive or injurious effects. While the US has asserted in a report to the UN that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack,"[4] it has not indicated which sorts of disruptive activities would qualify.

**International Humanitarian Law (IHL) (Jus in Bello)**

Cyber operations conducted by belligerents against each other after the initiation of "hostilities" or a "declaration of war" are regulated by the relevant *jus in bello* provisions, whether or not kinetic hostilities occur. This body of international law regulates *how* hostilities may be conducted in armed conflict and *protects* those affected by them. The international treaties that are relevant are the Geneva and Hague conventions as well as customary international legal principles of distinction, necessity, humanity, and proportionality. It is worth noting that declarations of war have not been issued in any recent conflict. The very notion of "war" as an international legal concept has been replaced by the term 'armed conflict'. In the information age, declarations of war are even more unlikely to occur. Requiring a declaration of war would appear to be unrealistic as it is not reconcilable with the surprise and plausible deniability factors that constitute two of the main advantages of cyber operations.

Cyber operations, however, executed in the context of an armed conflict (both international and non-international armed conflict) are subject to the law of armed conflict. For example, because the conflict between Russia and the Ukraine is international in character, the ensuing cyber operations are subject to IHL. According to the International Committee of the Red Cross (ICRC), the 'means and methods of warfare which resort to cyber technology are subject to IHL just as any new weapon or delivery system has been so far when used in an armed conflict by or on behalf of a party to such conflict.' The ICRC has noted that all parties to a conflict have an obligation to respect the rules of international humanitarian law if they resort to means and methods of cyberwarfare, including the principles of distinction, proportionality and precaution. The 2015 UN GGE report also noted

[4] Rep. of the Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/66/152, at 18 (July 20, 2010).

that the customary legal principles of IHL, humanity, necessity, proportionality and distinction apply in cyberspace.[5]

The question remains, however, as to whether isolated cyber operations between states without concurrent traditional hostilities will be regarded as amounting to an armed conflict, thereby triggering the laws of armed conflict. In other words, can cyber operations along constitute armed conflict? This question will probably be determined only through future state practice. Even the team of experts for the Tallinn Manual were unable to find agreement on this question. Providing some relevant insight on this question, the *Nicaragua* Court held that "clearly, use of force may *in some circumstances* raise questions of [IHL] law," implying that not always does a use of armed force amount to an armed conflict and thus trigger the application of *jus in bello*. For example, the mere supplying of arms to rebels does not bring about a state of war in the material sense. However, if a state not only armed the rebels but also trained them, it would be 'waging war' against the state fought by the rebels. Furthermore, other violations of Article 2(4) of the UN Charter, such as measures involving the threat but not the use of armed force (quarantine) also do not initiate, in themselves, an international armed conflict.

The Tallinn Manual accepts this view, stating that '[a]n international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more States,' where 'hostilities' is intended as 'the collective application of means and methods of warfare.' In order to qualify as a 'means of warfare', for example, any software deployed must be able to 'injure the enemy.' According to Michael Schmitt, who was the project director of the Tallinn Manual, IHL 'applies whenever computer network attacks can be ascribed to a State, are more than merely sporadic and isolated incidents and are either intended to cause injury, death, damage or destruction (or analogous effects), or such consequences are foreseeable.' The question is unsettled as to what level of damage must be met to trigger an armed conflict. For example, there is no consensus as to whether cyber operations resulting in severe non-destructive and non-injurious consequences can qualify as hostilities.

For the customary rules of proportionality and the requirement to take certain precautions during an attack, the meaning of the work 'attack' for purposes of cyber operations is contested and yet critically important to determining if the rules apply. Much debate has taken place among scholars and the Tallinn Manual experts on the issue, with no unanimous agreement. The question is whether the term "attack" is limited to that which causes physical harm to persons or intangible objects or whether is applies to acts of interference with the functionality of an object. The question of how states will realize the protection of certain objects or persons from cyber operations in an armed conflict is likely to develop over time. It is unlikely

[5] List of the 20 states in the 4th UN GGE: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Republic of Korea, Russian Federation, Spain, United Kingdom of Great Britain and Northern Ireland, United States.

that any international agreement will be developed on the issue of banning any cyber operations against civilian activities or data especially when non-destructive psychological operations directed at the civilian population are lawful in traditional kinetic conflict. Indeed, for cyber operations that only cause inconvenience or interference with non-essential services it would be difficult to get international agreement on such a ban. However, states in practice may begin to treat cyber operations against *essential* civilian services and data (financial services) as 'attacks' under LOAC, refraining from targeting them and condemning those that target them. In this manner, state practice may develop into customary international law over time. In other words, state practice will ultimately determine which specific civilian services and data will qualify as essential and therefore off-limits during conflict.

**Conclusions**

The international laws related to use of force and armed conflict were developed at a time when cyber operations were not even a thought in the minds of the drafters of the relevant treaties. When these rules were promulgated states did not have the capability to carry out cyber operations such as today. Today, however, cyber capabilities proliferate and states view them as force multipliers. These capabilities, however, also represent vulnerabilities for these states that rely on ICTs. Modern warfare has highlighted the need for these international laws to accommodate such capabilities within the law while ensuring that the object and purpose of IHL is protected during hostilities.

With this point in mind, I will offer a couple of thoughts as to where international law may be evolving in the context of cyber operations and the potential role for the US in the development of that law to ensure that the future legal landscape matches with the national security needs of the nation. To start with a claim, there likely will not be a new treaty codified that covers all aspects of the use of cyber operations under international law. In fact, since the path to negotiating any such treaty would be an arduous one, it is likely a waste of time, in my opinion, to attempt to arrive at such an agreement. Customary international law, however, can develop over time through state practice.

Customary international law evolves as states make claims about what they believe the law *is*, and *does,* in specific areas. Verbal acts such as diplomatic statements, policy statements, press releases, military manuals, decisions of national courts, opinions of official legal advisors, pleadings before international tribunals and executive decisions and regulations can all serve to develop international law. The US can actively work to develop those specific customary principles that it wishes to prevail internationally by being outspoken and transparent about what it views as the law in cyberspace. This, of course, will also require action consistent with words. Given the existing difficulties involved with adopting a new treaty, a reinterpretation of existing law to accord with the emergence of cyber operations along with the development of new customs that serve to adapt existing norms to cyber operations will likely be the path states take.

In this regard, it is paramount that the US government considers the importance of taking an active role in publicly setting forth its claims about how international law specifically applies to cyber operations or face the possibility that other states will develop the laws in a manner inconsistent with the interests of this country.

While it is difficult to predict whether any bright line tests will emerge in the areas of j*us ad bellum* and j*us in bello*, options for greater clarification of legal thresholds for cyber operations within this body of law exist. The US could articulate and promulgate an interpretation of the law it believes is applicable to cyber operations. For example, on the issue of what constitutes a use of force, the US could take the position that cyber operations executed against certain categories of targets, whether they are SCADA systems or specific critical infrastructures, creates a rebuttable presumption that such actions constitute "uses of force" for purposes of Article 2(4) of the UN Charter. The US could explicitly state such a position in a White House National Security Strategy asserting the legal thresholds for what would constitute a "use of force" and an "armed attack" in cyberspace. In making such legal assertions regarding thresholds, and acting in accordance with those outlined thresholds, the US could also seek agreement on these explicit thresholds from other states.