CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A Note on the Laws of War in Cyberspace

James A. Lewis

April 2010

There is some disagreement as to whether we can apply the existing legal framework for warfare to cyber conflict or whether a new legal framework is needed. This debate conflates two separate issues: can the existing legal framework be applied to cyber conflict and is the existing framework adequate. A review of the applicability of existing law of war suggests that if we approach cyber warfare as involving the use of a new technology to gain military advantage, the current body of international law can be applied to cyber conflict, but some issues involving sovereignty, combatants, "force" or "overflight"[1] may need expanded or new definitions or rules.

The legal framework for conflict applies to both state and non-state actors, but the decision as to when to apply it depends in large part on whether an action is deemed to have involved the use of force (e.g., it is an armed attack). Cyber conflict today almost exclusively involves crime and espionage. Crime is not an act of war, nor is espionage. Even reconnaissance in preparation for later conflict is not an act of war. The individuals and nations that engage in these activities do not think of themselves as engaging in warfare as international law defines it, and a lack of international norms for responsible behavior in cyber space reinforces the perception that this is not warfare.

We could begin to distinguish between a criminal act and an act of war in cyberspace if we defined an action in cyberspace that produced the equivalent effect as an armed attack as an act of war. One fundamental question is whether a cyber exploit must produce physical damage and casualties to be regarded as an act of force, or whether other, intangible damage inflicted outside of armed conflict can also be considered a use of force and an act of war.

Two separate bodies of law apply to cyber war: "jus ad bellum" – the laws governing a decision to resort to the use of force, and "jus in bello," the laws governing the conduct of hostilities. "Jus ad bellum" rules guide a nation's decision as to whether an incident justifies engaging in armed conflict or triggers the provisions of the UN Charter on a nation's right to use force in self-defense (the right of self-defense applies whether the attacker is a State actor or a non-State actor). The provisions of the UN Charter provide the legal framework for the "Jus ad bellum" and decisions on the use of force in self-defense are:

- Article 2, paragraph 4, which states that "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."

[1] Cyber attacks raise what can be called the "overflight" issue. Almost all cyber exploits require traversing third country networks to reach the target. Few states now have knowledge as to what passes through their territory, or what the intent of that traffic may be, due to the covert or clandestine nature of these cyber attack. Attacks are disguised as legitimate commercial traffic that is permitted to cross frontiers under existing commercial law and peering agreements among Tier 1 service providers. This could be interpreted as a violation of sovereignty unless the attacker asked permission to transit the network en route to an attack.

- Article 51, which states, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

To trigger the right of self-defense, national authorities would need to decide if a cyber exploit constituted an armed attack. A cyber exploit that was a violation of sovereignty is by itself not sufficient. An exploit that did not directly cause substantial death or physical destruction would most likely not qualify as an armed attack. The applicability of these provisions of the UN Charter will remain somewhat ambiguous, however, until it is possible to clarify when and under what circumstances, a disruptive exploit in cyberspace could be considered an armed attack.

The use of cyber attack is governed by "jus in bello" or the Law of Armed Conflict. These laws are derived from international conventions and treaties (such as the Hague and Geneva Conventions) and from customary international law. They set forth rules that govern the use of force during armed conflict. Three principles from the Law of War in particular establish a framework for judging the legality of using different forms of cyber attack during an armed conflict:

- The principle of distinction requires attacks to be limited to legitimate military objectives and that civilian objects shall not be the object of attack. Article 23 of the Hague Convention, for example, forbids belligerents "to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war."

- The principle of proportionality requires that the use of force in self-defense must be limited to that which is necessary to meet an imminent or actual armed attack and must be proportionate to the threat that is faced. Attacks on a military objective which cause incidental loss of life or injury to civilians or damage civilian property, in excess of that needed to obtain concrete and direct military advantage are prohibited

- The principle of discriminate attack prohibits attacks that cannot reasonably be limited to a specific military objective and which are indiscriminate or haphazard in their inclusion of civilian targets. Article 27 calls for belligerents to take all necessary steps to avoid damage to "buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes."

On their face, these legal principles would seem to prohibit attacks on purely civilian infrastructure when the resultant disruption or destruction would not produce meaningful military advantage (recognizing that there are no objective standards for determining what constitutes meaningful military advantage; these decisions are left to military commanders and a nation's political leadership).

Additionally, these principles imply that an attacker would need to assess the potential for collateral damage to civilian targets for a cyber attack to be lawful. To be consistent with the

laws of war, the use of cyber attacks during conflict would face the same constraints as attacks using kinetic weapons. The goal of the protections for civilians found in the laws of war is not to shield them from the dangers of military operations but to avoid capricious attacks undertaken solely to harm civilian targets.

Terror attacks are aimed at civilian targets and seek to create shock and fear to produce a political effect. Terrorists are not "lawful combatants" as defined by international law. Attacks against purely civilian by either state actors or non-state actors (such as terrorists) would be contrary to the laws of armed conflict, but the applicability of the laws of war to a cyber attack launched by terrorists would depend on the nature and duration of the attacks – a single attack could be considered a criminal act rather than an act of war; multiple attacks by the same group as part of a sustained campaign could justify the use of military force.

Some experts have argued that the prohibition on perfidy found in Article 37 of the Protocol Additional to the Geneva Conventions of 12 August 1949 also applies to cyber conflict. While the article prohibits "perfidy" (feigning incapacitation or non-combatant status, or a pretence of surrender), it allows for the use of "ruses" intended to mislead an adversary as long as the ruse itself does not violate the laws of war.

This brief review suggests that in most cases, existing laws for armed conflict can be applied to cyber attack, but that there are areas of ambiguity involving the violation of third party sovereignty, the use of cyber attacks by terrorists, and the amount and nature of damage from cyber attack that could be interpreted as an act of war. Some operational issues, such as the amount of prior assessment of collateral damage required to make an attack consistent with the laws of war are also unclear. There are as yet few precedents for resolving these ambiguities, but it may be possible to clarify them through further analysis or war games.