The Internet *in Bello*: Cyber War Law, Ethics & Policy

Seminar held 18 November 2011, Berkeley Law

Kate Jastram and Anne Quintin[1]

VII. Geography and Neutrality

The final panel session was chaired by Stephen Maurer. The speakers, in order, were Andrew Carswell and Eric Talbot Jensen. Given the interactive nature of both presentations, the points raised in discussion are included in the summaries of the presentations.

A. Comments by Andrew Carswell

Armed Forces Delegate, ICRC

Carswell observed that neutrality depends on borders, and borders depend on some concept of territory. If we take away the concept of borders, we do not have the concept of neutrality. However, it is not actually that straightforward in reality.

For one thing, the classification of conflict is no longer straightforward. It is regularly one of the more contentious issues at ICRC. So there is the law of neutrality, the classification of non-international armed conflict and international armed conflict, and then cyber. Non-international armed conflict has no concept of neutrality, legally speaking, thus presenting the question of whether and how we can draw parallels from international armed conflict.

He began with Hague Convention V of 1907.[2] One of most important things in this topic is that both the *jus ad bellum* and the *jus in bello* are engaged at the same time. The *jus ad bellum* framework is laden with politics. Logically, one side has breached the *jus ad bellum* for there to be a situation of armed conflict. The *jus in bello* is concerned with a completely different problem: will vulnerable individuals be protected? It is very important to keep the *jus ad bellum* and the *jus in bello* separate.

International armed conflict has a larger, more detailed body of applicable law than non-international armed conflict. Non-international armed conflict includes everything other than inter-State conflict. What about when non-international armed conflict conflicts spill over into other territory?

The law of neutrality applies *de jure* in an international armed conflict, but not in a non-international armed conflict. It regulates coexistence between belligerent States

[1] Kate Jastram is a Lecturer in Residence and Senior Fellow, Miller Institute for Global Challenges and the Law, University of California, Berkeley, School of Law. Anne Quintin is a Public Affairs Officer at the International Committee of the Red Cross in Washington, D.C.

[2] Mr. Carswell's power point slides on *Neutrality in Cyber War*, as well as a one page handout on Hague Convention V of 1907 are included in the Appendices.

and those not taking part in conflict. No declaration of neutrality is required. Hague Conventions V (land) and VIII (sea) are customary international law. The contemporary disagreement is on how to interpret them, as these laws have a slightly musty quality. It is necessary to look at State practice, as well as at the object and purpose of the Conventions.

The duties of neutral States are to refrain from participating in the conflict; to offer impartial treatment to belligerents, for example, the use of telecommunications equipment; to prevent belligerents from committing violations of their neutrality on their territory; and to intern combatants found on their territory until the end of hostilities, so that they will not re-engage in hostilities. The rights of neutral States are to continue normal diplomatic and trade relations, and to have their territory respected as inviolable.

The duties of belligerent States are to not move troops, weapons, and materials through neutral territory, including airspace and territorial waters, although there is a Law of the Sea exception if weapons are put away. Belligerents may not recruit corps of combatants from neutral States. The rights of belligerent States include a guarantee that neutral territory will not be used against them.

The consequence of a breach of neutrality is that the neutral State becomes a belligerent. If a belligerent State violates a neutral State, the latter can use self-defense to expel the belligerent.

Moving to consideration of the cyber realm, recall that 60% of Internet traffic traverses privately owned U.S. servers. How, then, can wired countries maintain neutrality during cyber conflict? The central issue: does the routing of attacks by a belligerent State through the Internet nodes of a neutral State violate its neutrality, and if so, what are the consequences?

There are four potential avenues for cyber-based violations of neutrality under Hague Convention V. The first would be using the cyber infrastructure in a neutral country's territory as a violation of that territory.[3] Launching an attack using a neutral country's server may be such a violation. Second, cyber means of warfare could be considered as "munitions of war" moved across a neutral territory.[4]

A third potential avenue is less likely, but cyber means could be considered 'erecting' or 'using' the belligerent's own communications equipment on neutral

[3] Hague V: 1. "The territory of neutral Powers is inviolable."

[4] Hague V: 2. "Belligerents are forbidden to move troops or convoys or either munitions of war or supplies across the territory of a neutral Power."
Hague V:5 "A neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur on its territory."

territory for military purposes.[5] Finally, cyber transmissions may be considered as a permissible use of a neutral State's telecommunications systems.[6] It depends on allowing both parties access. But it is unlikely that cyber warfare would be considered a permissible use.

Two examples illustrate these principles. As one example, consider a belligerent soldier sitting in neutral territory while physically launching a cyber attack. The solder has already violated neutrality simply by being in a neutral State. As a second example, the belligerent soldier sits in his own territory and launches a cyber attack via servers in a neutral country. Whether this is a violation depends on whether one considers it to be an attack in cyber space, or in the wires and servers in neutral territory. There is not a simple answer.

Another key issue is whether awareness of the belligerent's cyber means is necessary before the neutral State can be held responsible. If the neutral State does not know, can it be responsible for a violation of its duties of neutrality? Carswell suggested looking at the object and purpose of the law of neutrality. Is the neutral State's act or omission tantamount to participation in the armed conflict? If it is a violation, is it a severe or a fairly innocuous one?

Carswell recalled the distinction made by Col. Brown in his keynote address between cyberspace and cyber infrastructure. If cyber is its own space, we do not need to have a discussion about neutrality. To determine that, it is necessary to look at State practice. However, as noted earlier, State practice is difficult to ascertain since governments do not publicize their activities in this domain.

He then presented a hypothetical example to examine issues of neutrality in the context of a non-international armed conflict between the U.S. and a non-state actor (NSA). Assume NSA, which is fighting a non-international armed conflict against the U.S. in Alphaland, is commanding its branch in otherwise peaceful Bravoland to launch malware aimed at the U.S. Department of Defense.

Is Bravoland neutral? Not in a strict legal sense, since this is not an international armed conflict. Does Bravoland have an obligation to expel NSA or to deter the cyber

[5] Hague V: 3. "Belligerents are likewise forbidden to: (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea; (b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes…."

[6] Hague V: 8. "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

Hague V: 9 "Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents. A neutral Power must see to the same obligation being observed by companies or private individuals owing telegraph or telephone cables or wireless telegraphy apparatus."

attacks? What options are available to the U.S. if Bravoland fails to expel or deter? The answer turns on a more fundamental issue, which is the classification of the conflict. If the U.S. and NSA are in a global non-international armed conflict, NSA effectively takes the conflict with them wherever they go. Or, we can classify as ICRC would, which is that the U.S. and NSA are in a non-international armed conflict only within the territory of a State where the legal threshold is met (i.e., sufficient organization of the NSA and sufficiently intense hostilities with the U.S. within that country). On ICRC's reading, this is only the case in Alphaland.

If one does accept that IHL applies to the conflict between the U.S. and the NSA based in Bravoland, then conventional military force or a cyber counter-attack by the U.S. against Bravoland's NSA is not prohibited by IHL as such. However, in that case, the use of force against the NSA in Bravoland may or may not be prohibited by the *jus ad bellum* (this requires a separate analysis of UN Charter law). Again, we are looking at two separate bodies of law. IHL simply says attacks must be subject to distinction, proportionality, precaution, and so forth. If, on the other hand, IHL does not apply to this particular conflict, any force is limited to what is possible under international human rights law, or in a law enforcement framework, which is minimum use of force, lethal force only in self defense against an imminent threat of death or bodily harm, and use of force necessary and proportionate to the threat, not IHL proportionality. The answer depends how you view the whole framework.

In a variation of this hypothetical, assume that the NSA branch in Alphaland attacks a computer system in Bravoland, which then sends it across to the U.S. DOD without Bravoland's knowledge. There is not a simple answer. Is this a breach of Bravoland's neutrality? Can we draw parallels with law of neutrality between an international armed conflict and a non-international armed conflict? It is a very difficult question. If the U.S. wanted to use force against Bravoland computers, it would depend on a *jus ad bellum* framework. Examining neutrality in the context of cyber operations raises more questions than answers.

B. Comments by Eric Talbot Jensen

Associate Professor, Brigham Young University Law School

Jensen circulated a one page handout with two scenarios,[7] and offered a few caveats. First, he is involved in the Tallinn process and is drafting a manual dealing with how LOAC applies to cyber activities in international armed conflict, which he hopes to publish in one year with Cambridge University Press. The scenarios used in today's seminar will be published as part of an article set to appear in the *Fordham International Law Journal*.

He acknowledged that this is not a sophisticated scenario. It is not designed to hit the technological high points, but is adequate to highlight key points of neutrality law

[7] Prof. Jensen's handout is in the Appendices.

and how it plays out in international armed conflict and non-international armed conflict.

Scenario 1

Jensen's second caveat is that neutrality law by its text literally applies only in international armed conflict, so that is the setting for Scenario 1, an international armed conflict between State G and State X.

The second paragraph of Scenario 1 reads:

An agent of State G uses his tourist passport to lawfully enter neutral State H, carrying a cyber tool on a thumb drive. Once within State H, G's agent enters a cyber café and plugs the thumb drive into one of the computers. Upon activation, the cyber tool is copied to the hard drive and establishes a beacon that then awaits contact by another tool.

Jensen explained that the applicable law is Hague Convention V, Article 2.[8] Is the thumb drive with malware a munition? Has the agent of State G violated Article 2? There is no commentary to the Hague Convention. Is this what they were thinking? It is not completely clear. Jensen thinks it is a violation, so malware would be a munition. Does that trigger neutral State H's responsibility under Art. 5?[9] Jensen thinks it does.

The third paragraph of Scenario 1 reads:

Shortly thereafter, another agent of State G offers free thumb drives under the guise of a promotional gimmick from a local business to customers boarding a commercial cruise ship flagged in neutral State M, leaving from a port in neutral State R. Once the cruise ship leaves the port (and has likely entered the high seas), any customer who plugs the thumb drive into the ship's passenger computers will upload a malicious malware that will become resident on the ship's computer system. The ship's computers connect to the internet through a commercial carrier satellite operated by a company registered in neutral country F. Once the computer is connected to the internet, the malicious malware on the ship's computer sends a signal across the internet, seeking the beacon that is now resident on the computer in State H.

With respect to violations of neutrality, Jensen stated that at least for State R, it is the same situation. What about State M? Hague V would probably still apply. Is there an issue with neutrality? Clearly using a ruse? Does it result in killing or wounding? Is this a violation of M's neutrality? What is the role of private enterprises in a neutral State? There are the same issues as to State R, but when you get to State M, it is a bit

[8] Hague V: 2. "Belligerents are forbidden to move troops or convoys or either munitions of war or supplies across the territory of a neutral Power."

[9] Hague V: 5. "A neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur on its territory."

different. Customary practice, not found in Hague V, is to treat businesses as neutral also. So this would in fact be a violation of State M's neutrality.

He then turned to country F. Now there is a commercial satellite to upload malware from State M's ship. It does not really matter if this is on the high seas or not. Is the analysis with country F the same as with State M? Is there any reason to treat them differently? In Jensen's view, this concerns Article 8.[10] There are two approaches. One is to say this is about telegraphy. Another is to analogize. Article 8 says if it is normal public transit, country F does not have an obligation to police that. Belligerents can use that without violating neutrality.

The final paragraph of Scenario 1 reads:

Once the shipboard cyber tool has connected with the beacon, a code is executed which sends a malicious cyber program to the beacon. Upon arrival at the computer in State H, it combines with the cyber tool at the beacon and creates cyber malware that is then forwarded to a computer in State X to which State G has previously gained access. State G gained access to the computer in State X by hiring a citizen of neutral State J to create an access to a specific computer system in State X for the specific malware which State G created. Once the cyber malware reaches the computer in State X, it initiates an action that amounts to an attack on State X that causes death and destruction.

Jensen noted that one of the key points is that once it leaves the satellite of country F, it will traverse any number of neutral countries on the way back to State H. In this case, it is just Internet traffic. We have not invoked principles of neutrality. State G knows that when the malware is uploaded, it goes to country F's satellite. Bits and pieces will reconvene in State H. This is even less likely to implicate neutrality. Is a piece of the malware a weapon? It is not weaponized until it links with the beacon. You have a piece of gunpowder, and a piece of lead. The analogy breaks down. Perhaps Article 8 is not useful.

But note Article 9's applicability here.[11] Neutral States have to treat all belligerents equally. Then, here we are – is there anything different or unusual? At this point now, it is a weapon. We do know it is a weapon when it leaves State H and will do harm to State X. So here is State G, using a citizen of neutral State J. Does this implicate

[10] Hague V: 8. "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

[11] Hague V: 9. "Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents. A neutral Power must see to the same obligation being observed by companies or private individuals owing telegraph or telephone cables or wireless telegraphy apparatus."

just Citizen J, or State J? The law is Articles 16 and 17 of Hague V.[12] The citizen of State J is neutral under Article 16, but Article 17 says that once a neutral citizen starts to take action, he loses his neutrality. State J is neutral but Citizen J is not. If we want to be positivists, we have to allow some inequity in, and say it does matter if you cross a border rather than do it remotely.

In response to a question from the audience, Jensen said that he believes that if it travels over publicly available networks, it is not a violation of neutrality. He also noted that we want to encourage States to attack from their own territory; then, it is easier to trace it back. This will help preserve civilians from attack.

Scenario 2

Rather than international armed conflict between two states, assume a scenario where a non-State actor such as a terrorist organization, Non-State Actor G, takes these actions against State X.

Jensen pointed out that LOAC does not apply. What law does apply? This is a discouraging scenario. There is no applicable international criminal law. The domestic laws of State H and State X will apply if there are some, but this is a long drawn out potential process.

Moving through the various elements of the scenario, Jensen noted that on the cruise-ship, only the domestic law of the target state applies. With respect to the citizen of J, perhaps State J has a domestic provision.

His final point was that cyber is ubiquitous and pervasive where non-state actors have sovereign force capabilities. The law has created an incentive for non-state actors to take cyber actions, because they know that whatever law that catches up with them will be down the road, at some later time, and it may never catch up.

[12] Hague V: 16. "The nationals of a State which is not taking part in the war are considered as neutrals." Hague V: 17. "A neutral cannot avail himself of his neutrality (a) if he commits hostile acts against a belligerent; (b) if he commits acts in favor of a belligerent …."