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

Seminar held 18 November 2011, Berkeley Law

Kate Jastram and Anne Quintin[1]

II. Summary of presentations and recommendations

The main issues under consideration in the seminar were how *jus in bello* norms apply, if at all, to cyber security questions. Speakers thus addressed a wide range of legal, ethical and policy issues. "The Internet *in Bello*" is a timely topic. Much attention has been paid to *jus ad bellum* issues, examining when and under what circumstances a cyber operation constitutes an armed attack under United Nations Charter Article 51 for the purposes of self-defense. Yet relatively little discussion has focused on how cyber warfare might require new interpretations of rules, or even new rules, regarding the conduct of hostilities, or the *jus in bello*, once armed conflict has begun. Given the dizzying rate at which technology is advancing, it is important that experts in and out of government have the opportunity to share perspectives and identify questions to be addressed.

The seminar covered a number of themes across the panels and presentations. These included differing views on the significance of the issue itself and the applicability of international humanitarian law (IHL)/the law of armed conflict (LOAC) to cyber operations both generally and in terms of specific principles and definitions; U.S. policy challenges; the need for and obstacles to greater U.S. engagement with allies and others; the impact of high speed warfare on decision-making; and the unique role of the private sector.

The following commentary is summary in nature; the authors are responsible for any failure to convey the nuances of an argument or a discussion. Greater detail on each presentation may be found in Parts III-VII.

A. The significance of the issue and the applicability of IHL/LOAC to cyber operations

It is perhaps characteristic of the uncertainty posed by cyber capabilities in armed conflict that whether the issue itself is even significant was a matter of some dispute. From one perspective, cyber operations are a strategic development of first order significance. We are at the beginning of a revolution in military affairs, analogous to the dawn of the nuclear age. In addition to posing new threats, cyber may offer an unprecedented opportunity to comply with IHL/LOAC, particularly to the extent that it allows for "hyper distinction" between civilians and the military.

From another point of view, there is a great deal of "hype" associated with cyber security issues, much of it motivated by the profits to be made. There have been very few

[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.

examples of serious cyber attacks in the accepted legal meaning of the word. A recurring question of the day was whether "war" is in fact the correct characterization for most hostile cyber activity, and therefore whether the law of armed conflict is the relevant legal framework. The cyber security debate is and should be wider than the military and the law of armed conflict. While the U.S. focus on cyber "war" was critiqued as ill-advised, it was also noted that other governments are emulating the U.S. in this regard.

As general propositions, it is important both to assert the applicability of IHL/LOAC to cyber operations in armed conflict and also to acknowledge that not all hostile cyber actions should engage this body of law. Specific principles and definitions are discussed below. There is certainly a sense of unease in contemplating the difficulties in analogizing from established international law rules to new and rapidly changing technologies. Cyber's lack of correlation to physical geography, for example, makes application of traditional rules problematic. While IHL is too limited to deal with the full range of cyber security activities, and cyber issues must be addressed in other legal frameworks, it is also the case that IHL needs to develop to respond to the capabilities and threats of cyber war. The most promising, and underexplored, possibility is the potential for a more humane method of warfare.

B. Insights on specific IHL/LOAC principles and definitions

With respect to a basic notion such as *attack,* it was agreed that cyber operations causing physical damage would constitute an attack under Additional Protocol I, Article 49.1.[2] However, there is disagreement regarding neutralization under Additional Protocol I, Article 52.2.[3] Some would say that it is also an attack, at least in the context of an armed conflict already underway. However, this position is not shared by others, who reject the notion that neutralization is an attack and point out that LOAC does not address acts short of violence.

There was also concern with imprecise use of terminology: many cyber "attacks" are simply exploitation, or espionage. While this usage should be avoided by experts, it is inevitable that the media and laypersons will not limit themselves to the precise legal definition any more than they do with terms such as "refugee" and "war" itself.

Turning to *attribution*, the discussion took an interesting path beyond the usual observation that attribution is exceptionally difficult in the context of cyber. It was suggested that response to a cyber operation may call for a lower level of attribution than is required in kinetic warfare, since the task is essentially trying to stop a machine rather than to kill a person. This appears to be a reasonable response to the differing characters of kinetic and cyber war. However, it also raises a question of the interchangeability of the computers involved. If stopping one machine is ineffective because other machines can carry on with the attack, it

[2] API:49.1. "'Attacks' means acts of violence against the adversary, whether in offence or in defence."

[3] AP1:52. "Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or *neutralization*, in the circumstances ruling at the time, offers a definite military advantage." (emphasis added)

would seem that ultimately the person or group behind the attack must be targeted, and the issues of attribution re-emerge.

On a different aspect of attribution, it was also noted that we do not yet know how deterrence is applicable in cyber, since we often do not know who is responsible for hostile activity.

Regarding the important issue of *direct participation in hostilities*, it was agreed that non-state actors are a particularly salient issue in cyber operations. In a vivid example, it was noted that anyone with a credit card can rent a botnet. In that regard, how should hacktivists be treated? Turning to the military side, it was queried what purpose it served to have military personnel wear their uniforms while pushing buttons from 7000 miles away.

It was also suggested that the military-civilian overlap is significant in cyber, with the intelligence community perhaps more likely to have the relevant skill set than warfighters for carrying out cyber operations. While this may be appropriate, it also raises the issue of the relevant legal framework and the orientation of the relevant actors.

With regard to *distinction,* it is well-accepted that the definition of a military objective is not dependent on the means and methods employed. However, perspectives vary from that point on. Concern was expressed that indiscriminate attacks and unforeseen consequences are potentially the most serious problem of cyber operations. In contrast, optimism was also expressed that cyber offers an enhanced ability to be "hyper distinctive." One example cited in that regard was Stuxnet, which was tailored to destroy its target and nothing else.

On the related issue of *proportionality*, it was urged that cyber may be the best way to minimize collateral damage. Some argued that cyber operations may be more compatible with IHL rules than are kinetic operations, and questioned the relative lack of enthusiasm on the part of the IHL community thus far for this potential advance in enabling protection of civilians.

The analysis of *neutrality* in the context of cyber is complicated because of the nature of cyber (for example, 60% of Internet traffic traverses privately owned U.S. servers), as well as the difficulty of conflict classification, and the lack of *de jure* neutrality rules in non-international armed conflict.

With respect to *perfidy,* it was argued that in the cyber realm, only a very rare set of events would rise to the level of prohibited perfidy. However, on an intuitive level, cyber warfare and perfidy seem closely linked. It is worth examining that intuitive reaction more carefully to see why the law does not comport with our instinctive understanding and if therefore new norms should be developed.

Finally, in looking at *precaution*, views diverge on the principle. From one perspective, precaution arguably imposes on States the obligation to choose less harmful means to achieve military aims; cyber may sometimes offer that option. But from another point of view, it is not

obligatory to use cyber simply because it would reduce civilian damage to the greatest degree possible.

C. The need for, and obstacles to, greater U.S. engagement with allies and others

There are important reasons to be concerned about underdeveloped U.S. policy in this realm. While some feel that at best a set of policies is evolving, others are unable to discern a serious effort on the part of the U.S. government to develop a serious cyber security agenda. Still others point to a significant tension in U.S. law and policy regarding cyberspace, due in part to the complications of the Title 10/Title 50 debate.

There is a felt need for the U.S. to engage in, yet not dominate, discussion with its allies. The risk is that the U.S. voice is overwhelming, yet is driven by essentially domestic considerations. There is a need for greater understanding, and a greater appreciation on the part of the U.S. that even its close allies have different perspectives.

There are obstacles to arriving at a common understanding. On a practical level, there is the challenge of dealing with classified systems. It is difficult to share information. It is also the case that the U.S. is not eager to engage in international discussions on cyber matters, due to a long line of multilateral diplomatic failures including for example the Kyoto Protocol and the International Criminal Court.

D. Cyber speed

Two important points were made in relation to the speed of cyber activity. First, it necessarily results in a diminished role for human decision-making. Reacting in cyber time essentially means autonomous decision logic.

Second, cyber speed implies an important impact on traditional notions of space and geography. The closer an event gets to a time duration of zero, the closer it is to a non-event.

E. The unique role of the private sector

The role of the private sector came up several times throughout the seminar. It was noted that financial institutions are investing heavily to protect their networks from being compromised. It was observed that corporations are protective of their information and do not trust each other with it, which presents an impediment to cooperation with the government and with each other.

There is a high degree of control of cyberspace by the private sector in the U.S. Differing conclusions were drawn from this. It was suggested that this was perhaps one reason for U.S. reluctance to engage internationally. But in contrast, it was argued that we have an advantage in being able to trust private engineers in the cyber world, thus presenting an opportunity for including them in multilateral agreements.

F. Recommendations for further reflection

In addition to the points noted above, it was expressed frequently throughout the day with respect to the "Internet *in Bello"* that there are more questions than answers. This is clearly a rich area for scholarship and debate, deeply informed by operational challenges. Some of the specific recommendations include those made by Sir Daniel Bethlehem, who urged that there be more open debate, as nuanced and as specific as possible. He underscored the necessity of thinking beyond domestic horizons and the need for close allies to engage more deeply.

With respect to a possible treaty, Abraham Sofaer suggested that we should identify areas appropriate for cyber regulation, including military matters. It would be useful to start with something modest, for example, the prohibition of certain types of conduct, and the promotion of law enforcement cooperation. It would also be a step forward to negotiate an agreement for truly private technical committees that could prevent the development of content regulation and protect human rights. In contrast, caution was urged by those who feel that it is too early for a treaty and that the subject needs more deliberation. In particular, the fast moving nature of cyber technology signals caution in moving toward an international legal framework.

Col. Gary Brown noted that there is a reluctance to make rules and to say yes, since caution in this novel environment is safer. He emphasized the need for standing ground rules, so that each situation is not unique. It would appear that IHL/LOAC norms provide at least the framework for such standing ground rules. Despite limitations on disclosing information to the public, it would seem that at least some of the situations and issues faced by Cyber Command could be discussed in general terms with interested scholars and practitioners such as ICRC, perhaps in closed sessions.

The remainder of this paper summarizes the presentations in greater detail.