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

Seminar held 18 November 2011, Berkeley Law

Kate Jastram and Anne Quintin[1]

[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.

I. Introduction

This paper sets forth the proceedings of a seminar on "The Internet *in Bello*: Cyber War Law, Ethics & Policy" held at Berkeley Law School's Miller Institute for Global Challenges and the Law in Berkeley, California on 18 November 2011.

Part II of this paper summarizes the main issues raised and makes recommendations for further scholarship and inquiry. The remainder of the paper provides a more extensive rendering of each presentation and the ensuing discussions. Thus, Part III sketches the opening remarks of David Caron. Part IV covers the first panel on "the best defense", with presentations by Michael Nacht, Sir Daniel Bethlehem, and Abraham Sofaer. Part V summarizes the second panel on attack and distinction, with presentations by Anne Quintin, Lt. Col. Peter Hayden, and Sean Watts. Part VI reports on Col. Gary Brown's keynote address. Part VII concludes with the final panel on geography and neutrality, with presentations by Andrew Carswell and Eric Talbot Jensen. Additionally, a number of appendices are attached, including the seminar program, speaker biographies, handouts, links to recent relevant articles by the speakers, and a selected bibliography.[2] Finally, in order to reach out fully to those who were not able to be present, audio of the entire seminar is available online.[3]

The seminar was made possible by the support of the International Committee of the Red Cross, Berkeley Law's Miller Institute for Global Challenges and the Law, and the American Society of International Law's Lieber Society on the Law of Armed Conflict.[4]

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

---

[2] Further information can be found on the Intercross blog on *Why cyber war law matters* featuring Eric Talbot Jensen, at http://intercrossblog.icrc.org/blog/why-cyber-war-law-matters (last visited 23 March 2010) and in a radio story aired on 29 Nov 2011 on PRI's The World, *Making the Rules of Cyberwar,* by Matthew Brunwasser, available at http://www.theworld.org/2011/11/cyberwar-berkeley/ (last visited 23 March 2012).

[3] http://www.law.berkeley.edu/12032.htm (last visited 23 March 2012).

[4] The seminar was organized and chaired by Kate Jastram, who thanks Karen Chin, Eric Talbot Jensen, Anne Quintin, and Spenser Solis (Berkeley Law '13) for their assistance. The seminar was an expression of an ongoing collaboration between ICRC and Berkeley Law, part of the ICRC's initiative to encourage teaching and scholarship on international humanitarian law in U.S. law schools, as well as the interest of Berkeley Law's Miller Institute in providing a forum for scholars and practitioners to reflect upon and advance thinking in critical areas of international law.

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 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.[5] However, there is disagreement regarding neutralization under Additional Protocol I, Article 52.2.[6] 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 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.

---

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

[6] 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)

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.

III. Opening Remarks by David Caron

C. William Maxeiner Distinguished Professor of Law, University of California, Berkeley, School of Law; President, American Society of International Law

In his welcoming remarks, David Caron looked back to the founding of the American Society of International Law in 1906. Despite the development of new weapons and new practices in naval warfare, it was a period of optimism regarding the possibility for peaceful means, particularly arbitration or litigation, to provide an alternative to the use of force in the resolution of disputes. That optimism was shattered by the First World War, which set the course for the 20th century's many armed conflicts.

He noted that in this new millennium, hopes are again pinned on a new institution, the International Criminal Court, but we are again faced with new weapons and new challenges, including cyber warfare. Discussions within and between the responsible government agencies and others, including ASIL, are important in exploring how international law applies to these developments as well as in arriving at a common understanding of terminology. In a remark that was echoed by many speakers throughout the day, Caron observed that lawyers tend to try to think in analogies. For example, are drones like other weapons, or are they somehow special? Is this a new category, or is this part of a new category, and how do the old rules fit?

Before turning to the summary of the discussions, it should be noted that all of the seminar experts spoke in their individual capacity and did not necessarily represent the views of their current or former employers. While the presentations are attributed here, the discussions took place under Chatham House rules.

IV. Preparing the Battlefield: The Best Defense

The first panel was chaired by Beth van Schaack. The speakers, in order, were Michael Nacht, Sir Daniel Bethlehem, and Abraham Sofaer.

Van Schaack explained that the panel's role was to begin to outline the legal framework for engaging in and regulating offensive and defensive cyber operations. Panelists would focus on an armed conflict scenario, nevertheless keeping in mind that hostile cyber operations also often occur in peacetime, hence blurring the distinction between the two types of situations and the respective applicable legal framework. They would also focus on the interface with classic principles of IHL, or the *jus in bello*, including distinction, proportionality, neutrality, and direct participation in hostilities. Additionally, they would touch on the risk of cyber insecurity and the challenges of devising adequate responses, be they domestic or cooperative and multilateral systems, or international treaties. Finally, they would discuss the way forward, including where to take negotiations. In such a context of insecurity, account must be taken of countervailing imperatives, such as international human rights law, privacy concerns, and free speech concerns, which have interfered with our ability to come up with shared norms.

A. Comments by Michael Nacht

Thomas and Alison Schneider Professor of Public Policy, University of California, Berkeley

Nacht noted that he was responsible for developing national security strategy for Cyber Command while he was in the Office of the Under Secretary of Defense for Policy. He opened his remarks by stating that his focus was on U.S. national security policy and the manner in which it is shaped by law. He underlined, however, that each panelist had a different view of the elephant.

Nacht set out three elementary ideas by way of background: exploitation, defense, and offense. Starting with *exploitation,* or espionage, Nacht explained that the very nature of espionage was making it infeasible to develop codes of conduct, much less treaties, and hence to restrain it. But he also pointed out that exploitation is not just about damaging communications; it can have very direct military applications. For example, suppose the United States had a front-line, first-order weapon system, that is tested and ready to go, but has never been used or even fully deployed. Then suppose another government is able through *exfiltration* – a subset of exploitation – to take from the Internet the entire design parameters of the system, from the size of the Phillips screws to the most important elements of the stealth technology. That government's engineers could replicate the system, improve it, and then defeat it. This could have profound implications on the battlefield. Nacht warned that this was not a mere example; similar situations are happening, and indeed have happened already.

Nacht believes that we are in the infancy of cyber competition. He views it as analogous to the development of nuclear weapons in the late 1940s. It may not be that cyber technology will truly revolutionize our thinking about war the way nuclear weapons did, but it may come very close. It is the closest revolutionary development since nuclear weapons, far in excess of drones and other technical advances. The latter represent important tactical improvements, while cyber technology is a strategic development of first order significance. Exploitation is therefore a major issue.

Second, there are *defensive* aspects, which form the dominant area of public attention on cyber matters. The way we defend our assets, the technical fixes that are available, are questions of tremendous interest to a large technical community in Silicon Valley and elsewhere. Financial institutions, for example, are investing heavily to protect their financial networks from attack, including by hiring the best engineers and mathematicians from around the world.

Finally, the area that may be most important, although least talked about, is *offensive* capabilities. In the United States at this time, very little is said about U.S. offensive actions and capabilities, while there is a great deal of discussion about Chinese and Russian capabilities. For example, before Russia sent tanks into Georgia in 2008, it launched a cyber attack which completely disabled Georgian internal governmental communications, rendering the leadership in Tbilisi unable to communicate with their troops, their command structure, and parts of their diplomatic corps.

Such pre-operational cyber offenses will certainly grow as a general trend. Nacht indeed suggested that the next time a significant war begins, the first action may well be a cyber attack on the capabilities of the adversary. The United States has recently been engaged in several conflicts where the initial action was to use cruise missiles to destroy communications systems and air defense systems. The cyber option will be something considered not only by the U.S., but also by others.

Moving on from these three preliminary ideas, Nacht used his remaining time to comment on the eight elements set out in his article.[7] The eight core areas will remain central to our understanding and development of policy regardless of how technology evolves. In that regard, he observed that technology will evolve in a continuing revolutionary fashion, likely to render the technical issues discussed at today's seminar obsolete in five years.

1. *Declaratory policy*

What does the United States say about cyber war? What is our official policy? We do not actually have a policy now, rather we have an evolving set of policies. A core

[7] Nacht, "The Cyber Security Challenge," in UC Berkeley Goldman School of Public Policy *Policy Notes*, Spring 2011: 4 – 8, available at http://gspp.berkeley.edu/news-events/bpn_docs/PolicyNotes-2011Spring-web.pdf (last visited 23 March 2012) and in the Appendices.

dilemma for U.S. policymakers concerns the character and potential results of a cyber attack on the U.S. or its forces or allies such that it would rise to the prospect of a kinetic use of force response against the adversary. For example, would exfiltration of important data reach that threshold? Would disablement of air traffic control systems? What about an East Asian crisis in which the Pacific Command is given an order by Washington not to send a carrier battle group to the South China Sea but to Bermuda because someone has hacked into the system? What constitutes an act of war against the U.S. and what does not? We have not made a public statement about it in any clear way, and it will be some time before we can.

Nacht shared an interesting anecdote on declaratory policy. When the Chinese government interfered with Google a few years ago, Secretary Clinton made a major statement, almost the first statement of a very high-level individual about cyber aside from the President's speech in spring 2009.[8] She said that if the communications systems connecting our national security leaders were attacked, this would be unacceptable and lead to all kinds of possible responses. Nacht's impression was that such a declaration, envisaging use of force as a possible response, may have been a somewhat *ad hoc* response by the Secretary, as the U.S. has not yet clearly established what would be an appropriate response. We do not have many contingency plans ready to be implemented should there be an attack of this kind. Declaratory policy is an area that requires a great deal of work.

2. Deterrence policy

Since the advent of nuclear weapons, deterrence has become a keystone of U.S. national security policy, particularly with respect to the Soviet Union during the Cold War, and even now. It is used and misused by government officials who do not always comprehend the precise nature of what deterrence means: the conveyance of a will and capability to respond in the event of an attack.

We do not have a full understanding of how, if at all, deterrence is applicable in cyber, especially since attribution is made extremely difficult because of the anonymity that characterizes it. There is a great deal of research on how to solve the attribution problem, but it is unclear when a breakthrough might come. The question of who should be deterred is also a problematic one, considering the multiplicity of actors that have emerged, including major governments such as China, France, Israel, Russia, the U.K., and the U.S., along with terrorist groups, criminal elements, and individuals and groups of hackers and hacksters with a variety of motivations, or no motivation at all. It remains to be discussed how deterrence applies to cyber, and what U.S. policy should be.

---

[8] *Remarks on Internet Freedom*, Secretary of State Hillary Rodham Clinton, The Newseum, Washington, DC, Jan, 21, 2010, at http://www.state.gov/secretary/rm/2010/01/135519.htm (last visited 23 March 2012).

3. Authorities and responsibilities

U.S. cyber space is characterized by a complex web of actors including Cyber Command, the Department of Defense, and other units of government that are less well-developed. It is important to note that the military is responsible for defending only the dot mil network, which is a rather small network, and not the dot gov or the dot com networks. Therefore, the government is looking at only a tiny percentage of what is to be protected. The Department of Homeland Security is responsible for defending the dot gov network, but has only a very minimal capability to do so. Every government agency has its own cyber problem.

Because of Congress' involvement, oversight is another core area. Cyber is probably one of the only growth areas of the U.S. defense budget over the next five years. It is an infinite process, never quite resolved, so that determining authorities and responsibilities is an ongoing struggle.

4. Civil liberties issues

This is a very significant subject, especially when the power is in the hands of the Central Intelligence Agency and the military, causing many civil liberties organizations to fear a concentration of capacities.

5. Oversight

Oversight, especially the role of Congress, remains unresolved.

6. International consultations, negotiations, agreements

Basic questions are open: To whom do we speak? What do we say? What do we learn from them? Could there be codes of conduct or international treaties?

7. Cross-domain deterrence

We use it all the time, and we are beginning to think through all these issues.

8. Strengthening private sector – government cooperation

How can the government interact with the private sector effectively? How can the private sector help the government? These questions do not have simple answers. Corporations are protective of their information, and they do not trust each other to keep secrets. There is a great opportunity for improvement in communications.

B. Comments by Sir Daniel Bethlehem

Scholar in Residence, Columbia Law; 20 Essex Street Chambers; Legal Policy International Limited

To underscore the timeliness of the seminar, Bethlehem drew attention to four recent news items that touched upon the topic of cyber.

1. The first was a speech given by Vice President Joseph Biden on 1 November 2011 before a cyber conference convened in London by United Kingdom Foreign Secretary William Hague,[9] where he observed that "existing principles of international law apply online just as they do offline," and referenced proportionality and distinction.
2. The second was an interview with General James Cartwright, recently retired as Vice Chairman of the Joint Chiefs of Staff, on 6 November 2011.[10] General Cartwright insisted on the necessity of talking about our offensive capabilities and training to make them credible. This goes to issues of deterrence.
3. The third was an op-ed piece by Iain Lobban, director of the U.K. Government Communications Headquarters, in the *Times* of London on 31 October 2011,[11] where he identified very significant cyber threats and attacks that the U.K. has been facing, both in respect of the dot gov and the dot com infrastructure.
4. The fourth was a speech given by U.K. Foreign Secretary William Hague a few days prior to today's seminar on the importance of secret intelligence in foreign policy.[12] The speech did not touch directly on cyber, but provides a broader framework within which secret intelligence including cyber operates in the foreign intelligence sphere.

Bethlehem then addressed three preliminary points, as set out in the *Outline* he circulated.[13]

First preliminary point

Not all 'hostile' cyber actions properly engage or should properly engage a *jus in bello* analysis. In the same way that minor kinetic incursions do not trigger physical attacks, minor cyber incursions do not necessarily trigger Internet attacks; in both cases, applying a law of armed conflict (LOAC) framework might be too limited an answer. In terms of territory for instance, while armed conflict tends to be geographically circumscribed, this may not be so with a cyber attack. Similarly, not all cyber action occurring within the geographic space of a "hot" battlefield engages or should engage

[9] The London Conference on Cyberspace, 1-2 November 2011, at http://www.chathamhouse.org/research/international-security/current-projects/london-conference-cyberspace-1-2-november-2011 (last visited 23 March 2012).

[10] Andrea Shalal-Esa, Ex-U.S. general urges frank talk on cyber weapons. 6 November 2011, at http://www.reuters.com/article/2011/11/06/us-cyber-cartwright-idUSTRE7A514C20111106 (last visited 23 March 2012).

[11] "GCHQ chief reports 'disturbing' cyber-attacks on UK", London *Times*, 31 Oct 2011, http://www.bbc.co.uk/news/uk-15516959 (last visited 23 March 2012).

[12] "Securing our future: 16 November 2011, Foreign Secretary William Hague spoke about the role of secret intelligence in foreign policy in a speech", http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=692973282 (last visited 23 March 2012).

[13] Sir Daniel Bethlehem, *Outline of Remarks*, 18 Nov 2011, in the Appendices, with the disclaimer that this is a draft outline for discussion, and does not necessarily reflect his own settled views.

jus in bello analysis. For example, if cyber action is resorted to against drug barons in Afghanistan, or against Somali pirates, it does not automatically fall under the LOAC framework, although both countries have an on-going armed conflict on their respective territory.

Turning to the question of what type of cyber action should properly engage a *jus in bello* analysis, Sir Bethlehem suggested six elements of a threshold analysis that one should consider before deciding the appropriate answer.

1. Does the action have kinetic effects or does it have the potential to result in kinetic effects, such as destruction or injury?
2. Does it result in non-kinetic injury?
3. Is it in support of conventional military operations?
4. Is it intended to or could it degrade military capabilities?
5. Does action intend, or have the potential, to cause large-scale economic or similar damage?
6. Can it be attributed with a reasonably high degree of certainty?

One consequence of the above approach is that we should be excluding too hasty a resort to an IHL framework, simply because there is a hot conflict, or because the *jus ad bellum* is engaged, or because the action targets military infrastructure. Consider, for example, a hypothetical cyber attack that removes one penny from each U.S. Department of Defense check that is paid out. Would such an attack engage an IHL framework?

Second preliminary point

Even amongst allies, the world and the applicable framework look very different. For example, the United Kingdom is party to Additional Protocols I and II, as well as the European Convention on Human Rights, while the United States is not. The two countries have differing views on the extraterritorial application of human rights law, and each has its own domestic legal framework.

Consequently, if the U.K. and the U.S. were to have a conversation on cyber, it should first be ensured that they can work together. Interoperability of legal standards is needed; however, such a common understanding does not yet exist, and there is a real risk that the whole debate about cyber and IHL is driven by an American voice. Bethlehem then added an important recognition for U.S. audiences, sharing his sense that the U.S. debate on cyber is fundamentally driven by three appreciations. First, as mentioned earlier, is Secretary Clinton's speech on cyber, which was essentially a First Amendment speech. Second, and third, are the dueling issues of competence between Title 10 and Title 50, that is, between a military and a covert framework. These considerations drive the debate on authority, on framework, on resources, and on foreign and domestic authorizations. The rest of world may view it entirely differently, and it is important for the U.S. to engage.

By comparison, the U.K.'s authorization for intelligence agencies is based on the Intelligence Services Act of 1994, which is not a military act. There are fewer or different issues of the domestic/international divide. It is important that there is at least some broadly common analytical framework, at least among allies. We need some shared vision.

Third preliminary point

What are the sources of international law? In terms of treaties, IHL tends not to be weapon specific. Turning to customary international law, it is very difficult to determine what is customary in the cyber field as State practice and *opinio juris* are still insufficiently developed. In any event, all government lawyers tell their clients that just because something is legal does not make it wise.

After these three preliminary points, Bethlehem raised a number of issues related to process and to substance that responded to the panel title of preparing the battlefield. By way of an introductory comment to this portion of his remarks, he recommended looking at the Lawfare response to General Cartwright's interview he had previously mentioned.[14]

Issues (1)

Turning to systems and processes, he noted the challenge of dealing with classified systems, which makes it difficult to speak about cyber in detail and with a degree of specificity. In this respect, it is easy to say too little or too much.

Direct participation in hostilities also raises some difficult questions. Unlike U.S. Ft. Meade, the U.K. General Communications Headquarters is not only a military facility.

The next question then relates to the actual cyber weaponry. Is it a "fire and forget" weapon, or are there cascading effects? If these questions cannot be answered with clarity, how can an IHL assessment be planned and carried out?

Finally, cyber is quintessentially strategic, but it is also operational. In that regard, questions related to interoperability and the ensuing law of state responsibility may also be triggered. For example, what law would govern the actions of a British soldier embedded with U.S. forces in Afghanistan? Given a command that might under U.K. law engage European Convention on Human Rights responsibilities, how should the soldier respond? The law of complicity may also be engaged.

[14] Jack Goldsmith, "General Cartwright on Offensive Cyber Weapons and Deterrence", http://www.lawfareblog.com/2011/11/general-cartwright-on-offensive-cyber-weapons-and-deterrence/ (last visited 23 March 2012).

Issues (2)

We ought to address the following questions. Are there new appreciations of imminence, threats, and attacks in the sense of UN Charter Article 51? How should we analyze provenance and attribution? Is cyber inherently more IHL compatible?

Concluding observations

Bethlehem concluded by querying how we as lawyers can deal adequately with the framework of cyber law when it is so difficult to have the discussion even in Congress or Parliament in a nuanced manner. Emphasizing the importance of carefully informed State thinking, he put forward four proposals:

1) we need more open debate;
2) the debate needs to take place at a level of nuance and with as much specificity as possible;
3) as we engage in this debate, we need to think beyond domestic horizons – obviously the U.S. is driven by the Title 10/Title 50 First Amendment debate but must also consider how it is viewed elsewhere; and
4) there needs to be a deeper discussion amongst close allies as to how we view the world.

C. Comments by Abraham Sofaer

George P. Schultz Senior Fellow in Foreign Policy and National Security Affairs, Hoover Institution, Stanford University

Sofaer explained that his cyber-related work is largely aimed at cyber terrorism, but that he has also written on international agreements.[15] In his view, there is virtually a total lack of serious effort by the U.S. government to develop a serious agenda on cyber security. He noted that this was a quintessentially transnational problem.

He acknowledged that the current Administration has in fact adopted some international policies relating to cyber security, but cautioned the audience to keep in mind what we are constantly hearing, which is that we are the victims of a large-scale, on-going cyber war. U.S. Cyber Command was created precisely to deal with the military dimension of this war, and our efforts have resulted in massive expenditures.

He noted that cyber activities are a form of communication. Other forms of transnational communication are usually regulated by transnational agreements, for example, airlines, ships, and agriculture. Almost every transnational domain is coordinated by an international body. In contrast, cyber mainly belongs to the private sector. It began with technical experts in the U.S. who wanted to have more control over standard-setting, so that the government would not control cyberspace. Gradually, the experts have dominated that debate, although the government retains the root

[15] Abraham D. Sofaer, David Clark, Whitfield Diffie, "Cyber Security and International Agreements," *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy 2010,* 179 – 206, in the Appendices.

computer and power over the Internet Corporation for Assigned Names and Numbers (ICANN) through the Commerce Department. As a result, there is a high degree of control by the private sector.

But we are engaged in a different battle right now, one between governments to determine who is going to control cyberspace internationally. However, the U.S. has so far remained distant from that battle, for numerous and generally well-founded reasons. First, previous international negotiations, such as on the Landmines Convention, the International Criminal Court, and environmental agreements, have shown that the U.S. may not win this new battle. Second, the U.S. government is not at all enthused about international engagement in which it would talk about cyber standards and issues.

In parallel, some intergovernmental or private organizations, such as the Shanghai Cooperation Organization, are already trying to coordinate standard-setting. One of the issues at stake is precisely to ensure independence from a U.S.-dominated cyber world, and to create their own instruments. Similarly, the International Telecommunications Union has also asserted that it will be the leading global agency to set cyber standards. Taking into consideration these elements, Sofaer's report asks whether there is a role for international negotiations, and if so, what would be the best manner in which to approach them.

Cyber encompasses many issues, several of which are linked to the underlying fact that nations are competing for influence. Cyber weapons have been, and are being, developed for use in armed conflict, or for self-defense purposes. But what is surprising is the bitter reactions that cyber espionage and commercial theft have generated, even though they are but another form of espionage. They simply bring new means to pre-existing techniques. He cautioned that there is a great deal of hype regarding cyber and military operations.

Non-military issues are also at stake, as cyber also affects areas like commerce, the financial sector, or the energy sector. Standards have not yet been developed to protect these infrastructures. The White House is encouraging companies to cooperate, but that is not how the system works. To achieve security, there must be cooperation. Some members of Congress, including Senator Feinstein, are unhappy with the lackluster approach of the U.S. government.

Before going any further, it is important to identify areas of activity that are appropriate for cyber regulations. Instead of creating standards for anything and everything, we need to look at the types of measures that we would like to undertake, and create administrative structures to implement such measures. For the identification of such areas of activity, Sofaer referred participants to his paper.[16]

[16] Ibid.

What is important now is to work on military matters, and here he agrees with Sir Daniel Bethlehem. We already have treaties that deal with rules such as protection of civilians. How much further do we want to go? Do we want to allow combatants to disable healthcare systems, or civilian air traffic control? We want a convention to regulate cyber warfare.

The question now, however, concerns the available tools. Declarations of norms, objectives, and information-sharing procedures are among the tools that have been developed by the international community. However, cyber is a sensitive field; for instance, information-sharing remains difficult in cyber operations. This is why we should start with something modest: prohibit certain types of conduct, and promote law enforcement cooperation. Ultimately, we can address standards and practices, and then fashion the administrative structure. Eventually there will be an agency that regulates cyber weapons, just as there is for chemical weapons.

The issue then is whether we will take advantage of this, which would be one of most dramatic developments that we could actually bring about in international administration. We are uniquely in the hands of people we trust, that is, private engineers in the cyber world. There is a model in many international agencies of having not only States, and the Secretariat, but also technical committees with enormous influence. What if we could engage with, for example, the International Telecommunications Union? We could negotiate an agreement for truly private technical committees that will prevent the development of content regulation internationally, and will care about human rights advocacy, two things that the Shanghai Cooperation Organization is not doing. With respect to content control, there is a major contest going on. We are certainly working on defense, but Sofaer warned that we had better have two dimensions to our game.

D. Discussion on Preparing the Battlefield

A lively discussion at the conclusion of the first panel explored a number of important points, including U.S. reluctance to engage internationally versus the need for an international treaty; the need for deliberation versus greater dispatch in approaching international agreements; whose standards should govern; the utility and consequences of a war paradigm; and the application of IHL to cyber, in particular Stuxnet.

The need for an international treaty, obstacles thereto, shortcomings of

It was noted that a few regional or international convention either already exist, such as the Council of Europe Convention on Cyber Crime, or are in the process of being developed. For instance, the International Telecommunications Union and others are working on transnational organized crime, while the OECD is working on commercial aspects of the problem. Multilateral engagement is already happening and could be expanded.

One person agreed entirely that we need to engage better, and noted that cyber is multilateral. How does Thomas Friedman's observation that the world is flat translate into international law? There is a premium on doing things more thoughtfully, and on identifying areas for multilateral cyber regulation.

Another urged caution in the IHL field, arguing that it is too early to draft a treaty. Cyber is a compelling topic, but it needs more deliberation, and international organizations should not overreach themselves. The process of crafting the architecture should not be started without more of a shared vision. There is a need to talk among likeminded allies, to have common positions, for example, on content regulation. Building on the question of dueling domestic laws that had been noted as an important problem, a hypothetical was posed of Canada refusing to allow the posting of any material on a U.S. server that would be permissible under the First Amendment, if such material was illegal in Canada. Another concern expressed was that in law-abiding jurisdictions such as the U.S. and the U.K., governments will be subject to judicial review to ensure compliance with any international agreement, but non-state actors ("the bright kids") in other countries such as China will not.

Once we have common positions, it is beneficial to engage. Look at what China has been able to do without us. There is no way to prevent totalitarian regimes from making their own systems. By engaging we can set limits on what they do. They do want to stay in the commercial part of our world. The Internet is about commerce. It will be difficult, but the alternative of not engaging will have consequences.

Following up on the nuclear weapons analogy, one person pointed out that the first formal treaty on the subject was twenty-seven years after Hiroshima. The U.S. is still dealing with this issue today, as shown by a 2009 treaty with Russia. U.S. perspectives on the utility of large multilateral initiatives are not favorable, even in this Administration.

It was suggested that one reason for the U.S. government's reluctance to engage internationally may be the dominance of our private sector. One solution may be to consider private standards. It was also pointed out that we can engage in new thinking not only in terms of intergovernmental instruments, but also in the sense of protocols of agreement between internet service providers. Interstate law and traditional international law may not always be the answer. Such private agreements could even be discussed in collaboration with States.

However, another person challenged what he called the dubious view that the U.S. is "ahead of the game", a perspective which he described as the consensus of engineers in government agencies and research organizations in California. In his opinion, the European Convention on Cyber Crime is an excuse for not having a convention, since the parties to that agreement are all U.S. allies. None of our enemies

is party to that convention. In this person's view, we need serious mechanisms for developing agreed, operative standards, and so far, we are not ready to do it.

Utility and consequences of a war paradigm

It was suggested that a war paradigm could be counterproductive in dealing with cyber issues, since there had been greater international cooperation on terrorism prior to 9/11 and the U.S. "global war on terror". Concern was expressed that it might be a foolish mistake for the U.S. to focus on cyber "war". Responses to this observation were mixed. One person questioned the premise, arguing that there had actually been increased international cooperation between the U.S. and its allies regarding terrorism since 9/11. With respect to a possible U.S. mistake, it was noted that other governments are emulating our Cyber Command, realizing that this is a key component in competition in war. Furthermore, the establishment of a military component should not preclude an international dialogue. The two are not mutually exclusive.

The notion that a war paradigm was foolish was rejected by another person. The concern is not that this is the way cyber is framed but rather that it is tending to elicit a knee-jerk reaction and capture center ground. The debate is wider than just the military and IHL. There needs to be a more sophisticated debate.

In contrast, another person expressed agreement that cyber insecurity should not be characterized as "war." Not every ping is an attack. Why use the word "attack", which is a term of art? Some people do it from a profit motive. This person expressed his suspicions about the rhetoric of war, arguing that there were not more than ten real, serious, cyber attacks in the last decade. Shutting down the financial system of Estonia for two days, in this person's view, is not the kind of war that we are worried about.

Offensive actions

A question was posed regarding the use to which offensive cyber capabilities could be put. What are we building these tools for? In response, it was noted that much of this information is not available to the public. Instead, it is useful to consider Stuxnet as an example, although most agreed that this did not occur in a situation of armed conflict, nor did it create an armed conflict, but rather was used to further a policy objective. The Stuxnet virus was used to degrade Iranian centrifuges to slow down nuclear development, hence using offensive capability in the service of nuclear non-proliferation. There was, and is, no attribution of the attack.

In response to the question of whether Stuxnet was a good tool, it was suggested that the struggle of several U.S. Administrations and their attitude towards the Iranian nuclear program tend to show that the U.S. is seeking to avoid armed conflict with Iran. We are now in a situation of mostly sticks, and not many carrots. Stuxnet was a stick that did not lead to armed conflict.

In response to a question as to whether the use of Stuxnet was a violation of international law, one person drew the comparison that pursuing Osama bin Laden was a violation of Pakistani sovereignty. Policy is about weighing tradeoffs. Another person noted that if IHL rules do apply, it is going to be reasonably easy to determine the rules. The question is whether this is the right legal framework.

V. Attack and Distinction

The second panel was chaired by Kate Jastram. The speakers, in order of presentation, were Anne Quintin, Lt. Col. Peter Hayden, and Sean Watts.

Jastram began by noting that the shift to a discussion of *jus in bello* principles was not intended to close off the debate from the first panel as to whether this body of law applies. Indeed, examining how well the existing body of laws works in cyber operations is an important part of that inquiry. She recalled that attack is defined as an act of violence against an adversary, while distinction is one of the most fundamental principles of international humanitarian law. The panel would explore the applicability of these norms to the cyber domain.

A. Comments by Anne Quintin

Public Affairs Officer, International Committee of the Red Cross

Quintin observed that cyber warfare is a recent area of research for the International Committee of the Red Cross. With the military potential of cyber only starting to be explored, it is important to assert the applicability of IHL to cyber operations in the context of armed conflict. We do not yet know what the humanitarian consequences might be. However, this should not be a decisive obstacle, as we can already imagine the potential large-scale effects on civilian populations, if for instance airports, transportation systems, nuclear power stations, and dams were to be attacked. The consequences are difficult to assess now, but we cannot afford to wait until it is too late to prevent worst-case scenarios.

There is, of course, no mention in IHL of cyber operations, or computer attacks, or related terms. These terms do not have an internationally agreed legal meaning and are used in different contexts, not always limited to armed conflicts, and with different meanings. Does this indicate that IHL is ill-adapted to regulate such operations? The answer is no, for the following reasons.

First, new technologies have always been developed, and IHL is sufficiently broad to encompass them. Some specific conventions have been drafted for specific weapons, such as chemical and biological weapons, and anti-personnel mines. There may be a need for specific conventions on cyber weapons, but before they are developed, IHL does provide some answers.

The prospect of new types of weapons, not thought of and not conceivable at the time the Conventions and the Additional Protocols were drafted, is clearly envisaged in Article 36 of Additional Protocol I to the Geneva Conventions.[17] This clearly demonstrates that cyber operations, when conducted during an armed conflict, fall under the scope of IHL.

On a more practical note, if cyber means and methods produce the same effects as kinetic operations, they are – and should be – governed by the same rules. For example, a cyber manipulation of the air traffic control system resulting in the crash of civilian aircraft would be governed by IHL. The legality of such an attack would be assessed through the traditional principles applicable to kinetic operations -- distinction, proportionality, and precautions. There is no legal vacuum in cyberspace.

It is, however, important to stress that IHL comes into play only when cyber operations are committed in the context of an armed conflict. Which brings us to a second consideration: when do we have an armed conflict? What if the first or only hostile act is a cyber attack? Can this be qualified as constituting an armed conflict within the meaning of IHL? The answer today can only be theoretical. There is not enough State practice for a customary international law rule to be determined. But we do have a few elements of the answer.

Consider the definition of armed attack in Additional Protocol I, Article 49.1.[18] The term “attacks” means acts of violence against the adversary, whether in offense or in defense. "Acts of violence" have been interpreted as meaning physical force. Based on that view, which ICRC shares, viruses or worms which cause physical damage to persons or objects that go beyond the computer program or data attacked, could be qualified as an attack. To go further, it is not necessary to reach destruction or damage to have an armed attack. Additional Protocol I, Article 52.2 on military objectives also refers to neutralization.[19] Thus, it has been argued that neutralization is sufficient for an attack and so falls within IHL. Disabling a power grid, for example, without destroying it, would qualify.

Quintin then turned to the challenges posed by cyber operations to traditional notions of IHL, namely, *distinction, proportionality*, and *precaution*. *Distinction* requires parties to distinguish at all times between civilians and combatants, civilian objects and

[17] API: 36. “In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.”

[18] API:49.1. “’Attacks’ means acts of violence against the adversary, whether in offence or in defence.”

[19] AP1:52.2. “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.”

military objectives. It is sometimes claimed that cyber operations can be directed against a broader range of targets than kinetic attacks, including objects usually considered to be civilian objects. In ICRC's view, this claim is totally unfounded under IHL. The definition of a military objective is not dependent on the methods and means employed. The principle of distinction is entirely applicable during cyber attacks. It follows that attacks against civilian objects cannot be lawful, even if not leading to destruction.

To make distinction easier for parties, it has been suggested that one might verify the status of a data stream by distinctive markers, something similar to the marking of hospitals in kinetic warfare. So, for example, a computer facility could have a cyber marker to show that it is operated by a hospital. This is an idea that merits further discussion.

The principle of distinction also includes the prohibition against indiscriminate attacks. This is potentially the most serious problem in the context of cyber operations. Cyber space is characterized by interconnectivity. According to a recent Department of Defense report, DOD employees operate 15,000 computer networks with 7 million computers at hundreds of locations around the world. Nearly all military cyber infrastructure relies on civilian networks. As a consequence, the release of a virus against the military network could seep out into the civilian system of the targeted state, and could cross borders, and so would be indiscriminate. However, viruses and malware have reached a certain level of sophistication, allowing a high level of control over what is being targeted.

Therefore the question may rather be one of *proportionality*, as it is not possible to anticipate all the reverberating consequences. Using a concrete example of hospitals, "respect" means not only not attacking them but also not interfering with their work. In that regard, an attack against the military network that would also affect the network of the military medical services, for instance preventing them from continuing to give treatment to the wounded, would be disproportionate. But it should also be said that cyber attacks may also be the best way to minimize collateral damage. It may now be possible to switch something off instead of destroying it.

In considering *precaution*, parties are required to take all necessary precautions to reduce the effects of attacks. The obligation includes removing civilian objects from the vicinity of military objectives. In cyber space, the obligation becomes one of ensuring that military computer systems are sufficiently separate from the civilian network. But, as previously mentioned, information technology may also serve to limit incidental damage. It might be less damaging to disrupt than to destroy. Precaution arguably imposes on States the obligation to choose less harmful means to achieve military aims, and cyber operations may sometimes respond to that principle.

She concluded by confirming that ICRC will continue to follow cyber developments closely and to assess their potential humanitarian impact with a view to ensuring that IHL is respected.

B. Comments by Lt. Col. Peter Hayden

Deputy Legal Counsel (Operations), Office of the Chairman, Joint Chiefs of Staff

Hayden began with the disclaimer that he was presenting his own thoughts and was not speaking for the Department of Defense. He drew attention to a recent report in the *Washington Post* that DOD had advised Congress that it has the capability to conduct offensive operations in cyber space to defend the American nation, its allies, and its interests. If directed by the President, DOD will conduct offensive cyber operations in a manner consistent with policy, principles, and legal regimes the Department allows for kinetic operations, including the law of armed conflict.[20]

He noted that cyber is dangerous and exposes significant vulnerabilities, not least that we rely upon it so heavily, while it also offers tremendous opportunities in support of distinction and the concept of a military objective. With respect to the latter, he offered a comparison of the elements of the definition of a military objective contained in Additional Protocol I, Article 52.2 in the kinetic realm and in the cyber realm.

Nature In kinetic operations, it would be a tank. In the cyber realm, it is malware, key logging espionage malware, or something that could cause system failure. By nature, that is a legitimate military objective.

Location It can be a chokepoint, or high ground, or a bridge. In cyber space, it could be network nodes or key junctures.

Purpose and use It would be a pharmaceutical factory if it is manufacturing chemical weapons. In cyber, it could be many things. Michael Schmitt has noted that many things have a dual use in cyber.[21]

Cyber offers the opportunity to narrow the definition of a military objective with a greater degree of precision. "Military objective" is not a lawyer's creation, but a doctrinal definition for warfighters. Military strategic thinkers have adopted it straight out of Additional Protocol I; for instance, Milan Vego, a preeminent strategic military

---

[20] Ellen Nakashima, "Pentagon: Cyber offense part of U.S. strategy," *Washington Post*, Nov. 15, 2011, available at http://www.washingtonpost.com/national/national-security/pentagon-cyber-offense-part-of-us-strategy/2011/11/15/gIQArEAlPN_story.html?wprss=rss_politics (last visited 23 March 2012).

[21] Michael Schmitt, "Wired warfare: computer network attack and *jus in bello*," *International Review of the Red Cross*, Vol. 84, N°846 (June 2002) 365-98, available at http://www.icrc.org/eng/resources/documents/misc/5c5d5c.htm (last visited 23 March 2012).

thinker, included it in his work on *Joint Operational Warfare*.[22] The aim is to figure out what exactly is necessary to weaken the enemy forces to the greatest extent possible.

Hayden then presented the Stuxnet attack as a good illustration of what is possible under cyber and how to analyze concepts of military objective and attack. He stressed that all the information he had on Stuxnet was open source.

He recalled that in September 2010, a worm infected some 90,000 systems in several countries. After a while, it became clear that the worm was targeting Iran. More precisely, its aim was to get at a certain kind of programmable logic controller that ran centrifuges for a nuclear production facility in Iran. It targeted only those controllers which drove centrifuges manufactured by Siemens and which operated in certain parameters. Although Stuxnet infected 90,000 systems, most of them were not affected by it; Stuxnet simply replicated and moved on. Of nine thousand nuclear enrichment centrifuges, approximately one thousand failed, causing major damage and thus delaying Iran's nuclear production.

Going back to the concept of a military objective, Hayden used the hypothetical example of a hot war with "Antarctica", hence justifying the application of a LOAC framework. Antarctica's military objective is to degrade or take away Iran's nuclear capability. The subordinate military objective is to take down centrifuges. Subordinate to that is corruption of the programmable logic controllers.

Cyber can do only very limited things on its own: (1) alter a program's structure, or (2) give the program bad information. The first-level objective is to do something to the program or data, but the purpose is to cause physical destruction, breaking the controllers. So yes, this is probably an attack within the meaning of the law of war.

Under LOAC, the next question would be whether the attack violated other provisions. More specifically, did it cause incidental damage to civilians? There is a possibility that Iran's capacity to produce sufficient energy for its civilian population would have been compromised, in which case the attack could be considered to cause damage to the Iranian civilian population.

At this stage of the example, the hypothetical can be changed slightly: assume that among the affected centrifuges, some are used for military production and some are for civilian use. It is therefore a dual-use target. But Antarctica may have the ability to tailor its attack to avoid producing incidental civilian damage. To do that, Antarctica must have a great deal of knowledge about the enemy's systems. Cyber can allow those who use it to refine an attack and exclude harm to civilian objects.

[22] Milan Vego, *Joint Operational Warfare: Theory and Practice* (2007).

Another question that arises is how did Stuxnet get to Iran? The Iranian systems were spread out across the country, sheltered and hidden away. Moreover, they were air-gapped, not connected to the Internet. As a consequence, the attack had to be carried via thumb drives, which was a very clever way to defeat the strategy. Did the Stuxnet author cause incidental damage or loss to civilian lives? Antarctica would say no, there was no loss of civilian life or damage to civilian objects. The virus replicated through civilian systems without causing damage to them. At the end of the operation, it shut itself off, and eliminated itself. It was designed so as not to cause damage to any other system. It was a clever cyber weapon, almost as if it were written by lawyers.

Stuxnet is only one kind of model. There are all kinds of cyber attacks, due to the creativity of technical people. This is an area where offense probably has the advantage. What about the reverse?

Revisiting the issues from a defensive point of view, what could be done by Iran to stop Stuxnet, or Duku, the cyber missile that carried it, which is now also getting press? The carrier itself (the nodes through which it travels) is a military objective. Iran would want to disarm the enemy. It could destroy computers and nodes with a kinetic attack. Such an action would be destroying a *location*, and would need to follow the principle of proportionality. It could cause disproportionate damage given the number of systems the worm was spread across.

What if you could attack just the program itself, using bad data, or corrupting the program? Bytes would be fighting bytes, ones and zeros versus ones and zeros. What is interesting in that scenario is whether it amounts to an attack in the first place. As a piece of code that offers the enemy an advantage, there is no doubt that Stuxnet is a legitimate military objective. Michael Schmitt says military objectives can be defined only after there is an attack. Hayden would reverse that and say a military objective occurs once a warfighter sees a need to get rid of something that would offer him an advantage. Attack is one tool to neutralize. There are other tools – for example, psychological operations, and propaganda. If, for example, Berkeley was in a war with San Francisco, the Bay Bridge would be a military objective. Or you could get airport baggage handlers to go on strike, in order to shut down the airport. There are ways of neutralizing objectives that are not attacks under international law.

So if we can go after data, if we can attack programs or data such that there is no injury or loss of life to civilian objects, cyber allows us to be “hyper distinctive” in the context of war. We might be able to activate it only when pursuing military purposes.

He then raised the question of going into neutral countries, as attack vectors. That is a concern, as the law is undefined. With respect to the doctrine of neutrality, Hague Convention V of course did not mention cyber, so the law is not settled as to what happens when you go through neutral countries.

Cyber is a remarkable enabling tool. Hayden expressed a concern with Anne Quintin's earlier statement regarding the obligation to take precautions in attack. He suggested thinking of cyber as the Ferrari in the garage. Just because you have one, does not mean you always take it out of the garage.

Elaborating on this point, he noted that cyber attacks go after "zero day" capabilities. Once the target country finds out that there has been an attack, then everyone knows. Thus, cyber is the Ferrari in the garage that gets taken out only on special occasions. Cyber attacks are a perishable tool. The *Washington Post* reported that there was apparently consideration of using cyber attacks against Libya.[23] If so, one consideration would have been whether it was worth it. With cyber, losing your Ferrari is one factor in making that decision. Simply because you can reduce civilian damage the furthest by using a cyber capability does not mean that you have to use a cyber capability. You can husband the capability for a more opportune time. The reverse side of that point is that if you shepherd it too long, it will become obsolete, but that is not a legal concern.

C. Comments by Sean Watts

Associate Professor, Creighton University School of Law

Watts began by noting that cyber warfare offers a tremendous opportunity for lawyers to go through both longstanding legal concepts and terms of art, but also to move beyond doctrinal questions and think normatively about the law of war in ways that have been neglected for some time, for example, rethinking the fundamental balance between military objectives and humanity.

Watts has worked in the legal cyber realm on questions of status, and is interested in the way existing rules transfer to the cyber world. He particularly appreciated this panel for the opportunity to discuss the applicability, timeliness, and relevance of rules to targeting. His remarks would focus on a single dimension of attack, the notion of perfidy.

In its simplest terms, perfidy is a betrayal of legal good faith, consisting of three elements:

1) a feigned protected status;
2) an invitation to the target to recognize that protected legal status; and
3) a betrayal of that status, in order to take a military advantage.

These three elements, as Watts sometimes explains to his students, may be presented in terms of the elements of contracts: offer, acceptance and breach.

---

[23] Ellen Nakashima, "U.S. cyberweapons had been considered to disrupt Gaddafi's air defenses," *Washington Post*, Oct. 17, 2011, available at http://www.washingtonpost.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAETpssL_story.html (last visited 23 March 2012).

There is however a further legal understanding, or appreciation. Acts that might meet these three elements are not prohibited as perfidy unless they rise to a certain level. Traditionally, this result has to be killing or wounding of the enemy. Mere exploitation or damage of objects does not rise to this level. Additional Protocol I altered the traditional definition and added "capture",[24] creating two implications. First, a distinction should be made between perfidy and prohibited perfidy. Second, perfidy is a concept for combat, in the sense that it anticipates, like the legal notion of attack, a resort to violence.

As additional legal background, this is an area where codified law has rejected the general rule of staying away from examples. The prohibitions contained in Article 37 of Additional Protocol I clearly cite feigning wounds, feigning surrender or truce, feigning civilian status, and feigning neutral status. These are the protected classes of three out of the four Geneva Conventions. Another eye-catching characteristic of the Article lies in its partly-negative definition: routine military deception, ruses, and camouflage do not count as perfidy.

To finish up this legal snapshot, Watts explained the reason and purpose behind the prohibition of perfidy. The explication is complicated, and has ancient roots. In the earliest treaties, treachery was the term used, with "perfidy" emerging only in the mid-20th century. Treachery related to notions of military honor grounded in chivalry. Combatants had a right not to die by unfair or dishonorable means. By the mid-20th century, certainly by the 1970s, the object and purpose of the prohibition of perfidy is not to focus on combatants, but to focus on protected classes (the person whose status is being feigned). The logic goes like this: if soldiers are routinely exposed to feigned status, they will regard suspiciously and honor less frequently those protected statuses. Such an unfortunate consequence has been experienced in Iraq and Afghanistan. Battlefields on which civilian status is routinely feigned become very dangerous places for civilians. Finally, Watts added one last rationale behind the prohibition: belligerents must have some level of trust in each other in order for war to end. Repeated betrayal of trust jeopardizes chances for peace.

Perfidy in the cyber realm

Perfidy is an attractive way to explain what is troubling about cyber warfare. Cyber is sneaky, backhanded, and deceptive; like perfidy, it takes advantage of its target by appearing benign. On an intuitive level, cyber warfare and perfidy seem a close match. Watts found a confirmation of this intuition recently while attending events in Australia and in China. There were many questions regarding perfidy posed by very well-informed, well-placed, and – in a cyber sense – relevant actors.

However, not all cyber attacks amount to perfidy and thus violations of the law of armed conflict. It is necessary to move away from the intuitive reaction, and look at

[24] API: 37.1. "It is prohibited to kill, injure or capture an adversary by resort to perfidy."

the question more rigorously. Three observations may give us pause about that intuitive relationship.

1. Perfidy has always been expressed in human terms. Recalling the distinction between perfidy and prohibited perfidy, the prohibited type of perfidy features interaction between humans. One could envision a cyber attack that could satisfy the three elements, but the nonhuman cases are only a small fraction of these attacks.

2. Applied to cyber, perfidy loses much of its crucial interactive component. If something is automated, or preprogrammed, or based on algorithms, we lose that affirmative misrepresentation. It is much more implied, and difficult to analogize. There are cyber contexts that do involve human interactions, but they are reduced in the cyber realm.

Professor Caron was correct in his introduction – analogies seem to fail us. It is hard sometimes in cyber to make really useful analogies. A few questions then arise. When we lack this interactive component, do we really have offer and acceptance? To borrow contract thinking further, is there really a meeting of the minds that we envision in perfidy? If there is, is there a conversation that makes use of the legal terms relevant to perfidy, for example, a wounded person, or a potential prisoner of war?

3. Of course, perfidy exists. In the context of the *jus ad bellum*, these are the attacks that get all the press: the whole electrical grid, the whole air traffic control system. But Watts' understanding is that that is not the future of cyber attack. The future of cyber attacks are low intensity attacks, where you do not even realize that you have been attacked. It is below the defenders' threshold of reaction. All the defender knows is that he is a little more inefficient: things are not working well, but he cannot figure out why.

Catastrophic attacks in the future will be a rarity. Cyber space has a problem with perfidy, because prohibited perfidy is limited to attacks resulting in human death or injury, even if you can get over the legal definitional obstacle presented by attack, which Watts thinks is significant and is meaningful. Quintin shared with us a perspective articulated previously by Knut Doermann, that neutralization is captured in the prohibition on interactions with civilian objects.[25] Watts is more sympathetic to the view that there needs to be an attack before Additional Protocol I, Article. 52.2 is relevant. Be that as it may, we are dealing with a very rare set of events that can rise to

[25] Knut Doermann, "Applicability of the Additional Protocols to Computer Network Attacks", *International Committee of the Red Cross* (2004), available at http://www.icrc.org/eng/resources/documents/misc/68lg92.htm (last visited 23 March 2012).

the level required for prohibited perfidy. Watts concluded by noting that this portion of his remarks was a doctrinal sketch.

He then moved on to raise a few normative points: If this is the law, has the law of war not come up short? Maybe somehow it has missed something, if that is all we have. Perhaps the intuitive reactions are onto something. It is increasingly apparent that some of the law of armed conflict does not accommodate the significance of cyber. It is true when we apply the term "attacked." If a State is just exploiting or conducting espionage, it can get around IHL limitations. This is especially so considering that cyber stands to be opening shot of most future large-scale conflicts. Are those the first swirls of a downward spiral to unregulated warfare? If perfidy's purpose is to have some level of trust, we are setting the scene poorly.

In closing, Watts noted that he had presented a formalistic and skeptical application of perfidy to cyber. In spirit, perfidy does capture a great deal of what is troubling to us. But if the technical case for perfidy in cyber war is weak, how long will we tolerate the consequences of that gap? The positivist in him is not ready to concede that the law of armed conflict covers cyber war under perfidy. However, you can make a strong case under *lex ferenda* that this is where we need to develop the law.

D. Discussion on Attack and Distinction

It was clarified that Doermann's article[26] was not really looking at neutralization as the attack that could trigger armed conflict. But when you are in a situation of armed conflict, and you are using neutralization as a way to bring about a military advantage and can assert that this is targeting a military objective, it is difficult to say that neutralization is not an attack. There is a difference between neutralization as a first act, which is not enough to trigger armed conflict *per se*. But within the framework of armed conflict, it is different.

Another person responded that with respect to neutralization, Additional Protocol I: 49 says that an attack is violence against an adversary. It is repeated throughout the succeeding section. The *Commentary* also says that this is concerned with acts of violence. Neutralization may be inconvenient but it does not reach the level of a violent attack. LOAC does not address acts short of violence.

It was noted that speakers had emphasized cyber both as offering precision and as risking unforeseen consequences.

One person argued that obviously Stuxnet had spread all over world, but had activated only against its target. Cyber is potentially indiscriminate, but when you have programmers who are able to specify a certain set of conditions, it is possible to achieve two things at once. It can be sent out broadly, but defined as to when it will actually

[26] Ibid.

have an effect. Assuming that States can control what the tool will do, cyber tools are capable of precision effects, and can be the ultimate in discrimination.

One person then queried whether Stuxnet was representative of cyber warfare. In response, it was asserted that it was important to resist treating cyber attacks monolithically. Cyber is complex and always changing. Analogies and frameworks are hard to maintain. There is an understandable desire to generalize, but it is difficult to do so.

Another person wanted to emphasize a concern about using the word "attack" when talking about a violent act. If you look at cases from the International Court of Justice, an attack has to be significant to generate the right of self defense. There are proportionate measures permitted for lesser attacks. Most of so-called cyber attacks are exploitation. Most of the things complained about are efforts to get into computer systems, not to degrade them but to get information. Hacking fraud does not necessarily have any impact on a system. IHL has a very limited scope in cyber security. Most of it has nothing to do with the military.

One person agreed that he was enough of a legal formalist to adhere to that as well. Attack means different things in the *jus ad bellum* and the *jus in bello*. But, people call it a cyber "attack" for a reason. It is not all just the profit motive, as had been suggested in the previous discussion. "Attack" portrays more accurately what is at stake. This is again where analogies fail. When you lose data, or lose access to service – something more has been lost than the legal definition of attack suggests. It is just a normative point. If States are going to act like this is war, doesn't LOW need to expand and acknowledge this reality? It would be better to see something more principled.

VI. Keynote Address by Col. Gary Brown

Staff Judge Advocate, U.S. Cyber Command

Brown began with the disclaimer that he was presenting his personal thoughts only and was not speaking for Cyber Command or the Department of Defense.
He summed up Cyber Command's mission statement as consisting of three parts: operating the Department of Defense, defending the Department of Defense, and providing options to the President. Based on those options, Cyber Command operates mainly in defense; however, its actions may often be assimilated to offense, in the sense that effectively defending a network can require taking actions outside of that network.

He observed that analyzing cyberspace is difficult for lawyers. It can be frustrating to try to lay rule sets on cyberspace, while still learning how it works. It is also frustrating for the warfighters, as evidenced by Sean Watts' remarks on perfidy and chivalry.

Warfighters are accustomed to fighting from a position of danger. Cyber presents another stage in the evolution of non-heroic warfare, which also occurred with

crossbows, aerial bombardment, and unmanned aerial vehicles or drones. All of these pose(d) different kinds of combat, different sets of problems, and different sets of issues in looking for acceptance from combatants. He mentioned this because one of the issues facing the military now is the question of who is in charge. Warfighter skills do not necessarily translate into cyber warfare. Skills may translate more clearly from the intelligence community. The result can be a different mix and a different way of looking at warfare. There is significant tension in policy and law with respect to cyberspace.

His remarks would focus on three larger issues around which some other issues swirl. These larger issues are the interfaces between human and machine, between cyberspace and physical space, and between civilian and military.

1) The human - machine interface

One aspect of the human-machine interface is the level of attribution. Recalling his earlier comments on non-heroic warfare, he noted that this issue has already come up in the past. Where there was once face-to-face fighting, we have now moved further apart. Cyberspace takes this to a different level, but people have not yet accepted that there is a difference in the level of attribution.

When soldiers are firing back in a combat zone, they want to stop the machine – they are not too concerned about individual doing the attacking. But in cyberspace, when we suffer impermissible events however characterized, does it matter who that person is? What we would like to do is attribute it to a machine and make it stop. However, in the cyber context the person is usually not operating from his or her own machine. Should we not be able to stop the machine? That might be the way to look at attribution in cyber space. The goal in the kinetic world is to kill someone, which perhaps justifies a higher level of attribution.

A second aspect of the human – machine interface is the challenge of speed. Because of the speed of cyber operations, many analogies break down. Espionage has happened since time immemorial. But espionage in the kinetic world is limited to what can be stored in one person's brain, or file cabinet. In cyber, terabytes of information can be exfiltrated in just minutes.

Another challenge is that the rate of speed at which packets of information can travel the globe makes it difficult to keep humans in the decision loop. Could we end up with automated warfare? Humans will not have time to make decisions, and even if it were possible, the human would probably be a low-level officer who would need to go up the chain of command. By that time, the event would be over. Reacting in cyber time means autonomous decision logic. We will have to deal with this. To complete this thought, he noted that because of speed, there is an impact on space and geography. If a country sends angry ones and zeros across your border, you might think it infringes on your sovereignty. When a soldier goes across your border, the situation is clear with regards to the breach of sovereignty. However, the question still remains of a

soldier crossing your border for only one second, or for a half-second. The closer that number gets to zero, the closer it is to a non-event. Speed changes the equation.

2) The cyberspace - physical space interface

Cyberspace is not the same as the Internet. The Internet is a way to access cyberspace. We tend to speak of the Internet as synonymous with cyber, but the Internet is physical – routers, cables, terminals, etc. - while there are stand-alone networks not connected to the Internet. So we are at a disadvantage, since we are not sure what cyberspace is. The DOD definition includes terms not defined. William Gibson defined it as a "mass consensual hallucination."[27] We would like it to have strong correlation to geography. Nation-states, the Department of State, the Department of Defense, and international humanitarian law are organized that way. Yet now we have a brand new area of operations that does not fit well with geography.

The Internet sends one and zeros around as packetized bits of data, going in different directions and reassembling on another person's laptop. Tying cyberspace to physical geography has us tied in knots, and makes it difficult for us to answer questions. Often, things are occurring in U.S., but the U.S. military does not take action in the U.S. Does it matter if angry ones and zeros are passing through infrastructure located in the United States? Most people engaged in activities that we do not like do not care where things are located in physical space.

3) The civilian – military interface

There is a concern about militarizing cyberspace. The Internet is dual use. In the U.S., most concerns revolve around privacy. This is not true in information-sensitive societies, which are more concerned about their citizens' ability to see the Internet. For example, Secretary of State Clinton has spoken about systems in China. We spend money and effort to make sure we are not looking at data of U.S. nationals, and we are good at it. The result is that the *News of World* hacks into voicemail in the U.K., and criminals steal your bank data, but the U.S. government does not look at your information. For people who follow the law, the law is effective. However, the Internet is a freewheeling space. Because there is no effective enforcement mechanism, the law is irrelevant for those who do not care about the law. The nature of the Internet also makes it difficult to have a technological solution. Another issue of concern is the reality that privacy from government impacts the government's ability to protect.

More interesting than worrying about militarizing cyberspace is the role of civilians in military operations. There are interesting situations in IHL, namely, hacktivists. How should these civilians be treated? If they were members of the military, it would be a military operation. It is not unprecedented in IHL to have civilians engaged in war, but what is unprecedented is the nature of cyberspace, such as malware and recruitment by charismatic individuals, for example. Non-state actors are

[27] William Gibson, "Burning Chrome", *Omni* (July 1982).

more of an issue in cyberspace. They can communicate quickly and cheaply. Anyone with a credit card can rent a botnet. It is not necessarily lawful but it is possible.

He then raised the question of who is pushing the buttons. In kinetic operations, they are wearing military uniforms. In cyber, they are in a windowless room, 7000 miles away. He is just not sure it makes a difference if they are wearing uniforms. He is not certain that this is a helpful rule in cyber.

These are some of the issues that swirl around these three interfaces. Where does this leave us? There are not a lot of answers.

Generally in the U.S. and the rest of the cyber-advanced world, the debate has tended to focus on what we cannot do, as opposed to what we can do. Stuxnet had a kill switch to turn it off. In an article, someone said that that must have been suggested by lawyers – who else would bother?

Lawyers in cyber are almost indistinguishable from operators, because so much law and policy are involved in operations. But operators like to act, and lawyers like to talk. So there is a need for some standing ground rules, as opposed to each case being unique. There is a reluctance to make rules and to say yes. Cyber is unique, so the safe path is to exercise caution. However, the danger is missing an unprecedented opportunity to promote a more humane method of warfare. Kinetic is easier to understand, since we have hundreds of years of history. But successful military operations without people dying would be a good thing. It is odd that cyber has not gone further in the IHL world yet.

Another factor is that cyberwar may be too antiseptic; it may make war too easy. But with that we have come full circle. Operators are used to fighting from a position of danger. IHL is looking out for people. We want to lose the fewest lives possible. Now the military and IHL are switched around and mixed; the military is offering a solution with less collateral damage and casualties, and the IHL community seems concerned that war will become *too* clean.

These questions are worth asking. We are at the beginning of a revolution in military affairs. Applying policy and law to cyber operations is fundamentally different than applying them to more traditional operations. The challenges can be fascinating, frustrating, and fun. It is a great, exciting place to be.

A. Discussion following the keynote address

It was noted that there are two categories of cyber users: States who want to comply with law, and others who do not. The problem seems less a legal one than a technological one. Do we need more law?

In response, it was suggested that there is not an either/or answer. We should be careful to advocate law in this area. Address those who comply with the law, but do not foreclose a response to rogue groups. As for technological solutions, there is most likely not one. The solution would be to lay a new Internet, with different rules for users. The Internet is designed for reliability, not security. It is redundant. If we re-engineered it for security, with foolproof ID, that might be different. But what is foolproof? Even a DNA-based system could be hacked into. And, any system that made anonymity more difficult would likely result in less free sharing of ideas, which is one of the great strengths of the Internet.

There was some confusion over, and discussion regarding, the applicability of the civilian – military distinction, particularly the notion that the requirement for military personnel engaging in cyber operations to be in uniform was meaningless because of their remoteness from any physical battlefield. It was acknowledged that the interface is muddy between Title 18, Title 50, and Title 10. However, it was urged that we not put ourselves in a situation where in an emergency our hands are tied because we are not sure.

With respect to speed and automaticity, it was suggested that the main idea would be to frontload a response: "If these seventeen things happen, cut off Internet traffic from X nation." There are going to have to be some instances where the only human in the loop is setting the pre-determined response to a set of circumstances. Taking the time to pass notice up the chain of command would mean any reaction would be too late.

With respect to Stuxnet, one person noted that it did not result in death and queried if it was a violation of international law and/or an armed attack. In response, it was suggested that things that do not kill civilians are a better course of action. It is indisputable that it was effective; it slowed down the development of nuclear weapons. There is not a consensus on whether it qualified as an armed attack; that is still a matter of debate. A state of armed conflict did not exist at the time, so Stuxnet as an opening salvo might not meet the requirements of international law.

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.[28] 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 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.

[28] 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.

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.[29] 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.[30]

A third potential avenue is less likely, but cyber means could be considered 'erecting' or 'using' the belligerent's own communications equipment on neutral territory for military purposes.[31] Finally, cyber transmissions may be considered as a permissible use of a neutral State's telecommunications systems.[32] It depends on allowing both parties access. But it is unlikely that cyber warfare would be considered a permissible use.

---

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

[30] 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."

[31] 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…."

[32] 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."

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 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,[33] 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 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.

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

Jensen explained that the applicable law is Hague Convention V, Article 2.[34] 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?[35] 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 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.[36] 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

[34] 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."

[35] 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."

[36] 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."

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.[37] 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 just Citizen J, or State J? The law is Articles 16 and 17 of Hague V.[38] 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.

[37] 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."

[38] 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 …."

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.