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

Seminar held 18 November 2011, Berkeley Law

Kate Jastram and Anne Quintin[1]

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.

[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.

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."[2] 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

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

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 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.