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

Seminar held 18 November 2011, Berkeley Law

Kate Jastram and Anne Quintin[1]

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

[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.

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.[2] 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.

[2] 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.

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 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.[3] 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.

---

[3] *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,[4] 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.[5] 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,[6] 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.[7] 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.[8]

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 *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.

---

[4] 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).

[5] 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).

[6] "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).

[7] "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).

[8] 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.

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.[9]

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.

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

[9] 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).

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.[10] 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 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

[10] 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.

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.[11]

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

[11] Ibid.

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.