Panel 3: Applicability of International Law to Cyberspace & Characterization of Cyber Incidents

Catherine Lotrionte and Eneken Tikk, co-chairs

'Cyber security' and the acceptable behavior of state and non-state actors in 'cyberspace' has become one of the centerpieces of international and national security talks. Calls for new legal instruments have been placed with international organizations by some states while others call for application of existing legal frameworks.

Yet there is no 'cyber' framework *per se* from a legal perspective. There is, however, a substantive body of legal principles and norms, international and regional, to address different implications of uses of ICTs, such as how we establish and maintain relevant infrastructures, protocols and content; how we defend personal, corporate, national and international interests pertaining to uses of ICTs and how we balance interests involved under the contemporary paradigm of 'security'. Addressing 'the law of cyber security' therefore means addressing different legal authorities, instruments, concepts and practices some of which can and some of which cannot be applied simultaneously and all of which involve prerequisites to their applicability. Furthermore, these need to be addressed with the different national legal interpretations from various countries.

This panel addressed legal principles, instruments and concepts applicable to uses of ICTs and selected consequences of uses that do not rise to the threshold of 'use of force' and 'armed attack'. This panel outlined already existing normative approaches to telecommunications, crime/law enforcement, electronic transactions, privacy, espionage, etc and explained and discussed the relevance of such frameworks from state responsibility and government-level decision-making/strategy development perspective

The panel was structured to address:

1. The practical vs. political need for and rationale behind the requests for new international legal instruments (e.g. the Russian and Chinese initiatives of the Code of Conduct, Draft Convention of Information Security and the UNODC cyber crime treaty initiative);
2. A 'legal' versus a 'policy' assessment of an incident and the choice of responses and remedies;
3. Categorization of cyber incidents under existing legal thresholds;
4. Identifying (potential) gaps in existing legal instruments and practice to be filled in by other normative (including non-binding) frameworks.

Summary

Given the plurality of legal areas, regimes and instruments potentially applicable to cyber conflict in its various forms and stages, it is essential to clarify the basic definitions for the purpose of any deeper discussion. Where needed, it makes sense to define key terms so that lawyers with different background as well as non-legal experts would not talk past each other. For example, there is wide divergence on whether cyber attack on Estonia in 2007 rose to level of armed attack. While it did not rise to that level, strategic communications at government level used a lot of terminology from the law of armed conflict. This indicates that policy makers did not use those terms correctly which has had consequences to how people understand the situation and relevant legal remedies.

One must also be careful as experts with international relations scholars use the term 'norms' whereas lawyers speak in the language of laws and rules. The two are not the same.

By legal norms we mean legally binding rules. International law is made by states and comes from pre-defined sources – 1) treaties and conventions – legally binding written documents among the states; 2) customary international law – created by consensus of states – e.g. diplomatic immunity, anticipatory self-defense, state practice – continuous practice over a long period of time, under belief that they are legally obliged to behave in a certain manner; 3) general principles – rooted in domestic laws of member states, e.g. if a critical mass of nations have criminalized murder, it represents a general principle recognized among civilization; 4) writings and teachings of scholars.

While the discussion on the applicability of international law to cyber now seems to turn to how it applies, applying international treaties, customary law and established legal principles to factual scenarios is very complicated. The panel agreed in general with the applicability of international law to cyber conflict, emphasizing that an acknowledgment like this does not take us very far.

We used to ask if international law is sufficient to deal with these incidents. These discussions were often not guided by a comprehensive picture of all legal areas and instruments that are relevant to the whole spectrum of issues. In fact, international law covers a wide array of issues, including privacy, cybercrime, telecommunications, etc. At some point of our debate and strategy development, we need to bring these different areas together to apply them along the spectrum of cyber conflicts between states as well as non-state actors, including business and individual users.

The UN's core function is to deal with threats to international peace and security. So under its Charter UN could address such threats in cyber (the Security Council system applies). This does not necessarily tell us what the UN considers a threat to international peace and security from the 'cyber' perspective.

Focusing heavily on the UN Charter leads us to overlook other multilaterally agreed obligations that shape state behavior in or for conflict. We have norms that oblige states to offer secure information society services and therefore are markers for assessing the obligation of each potential victim to exercise care over their networks. We have norms that oblige everyone who processes personal data to provide a level of confidentiality, integrity and availability that corresponds to the risks associated with the sensitivity of such data.

In sum we have a number of internationally agreed norms that should shape our behavior and that should take us through the whole spectrum and address different aspects and stages of cyber

conflict or harmful behavior in cyber space. We have norms that are intended to prevent access by third parties (e.g. data protection), and we have norms that apply when it has happened (crime law). In parallel, we have the concept of state responsibility that applies in addition to individual obligations of service providers or network operators.

The panel then went on to discuss some topics of interest to the audience.

Sovereignty is a long established concept dating back to Westphalia. Every state is free from external forces interfering in its internal affairs. All states are equal under law regardless of their size or GDP. To control "what is yours" in a government's perspective is an established principle, and from a legal perspective a country has every right under international law to exercise its sovereignty to achieve its goals. How far the sovereignty can be exercised will, among other things, depend on the sovereign interests of other states. The principle of being able to control "what is yours" is a tenet closely guarded by states. But, international law recognizes need to balance sovereignty against other international principles like human rights.

States have chosen to give up sovereignty over time, based on consent. Legal practice has developed the concept of sovereignty to be weighed against certain commonly accepted values, such as human rights, and limited by consensus certain aspects of sovereignty. Such limitations cannot generally happen without state consent.

The obligations deriving from international law translate into state responsibility that includes the responsibility of a state for breaches of international law by those under its jurisdiction. 9/11 stretched that concept to extend the responsibility of a state to non-state actors it is unwilling or unable to control. 9/11 changed threshold for holding states responsible (Afghanistan and Al Qaeda). Principle of self-defense is also important in cyber, balanced against sovereignty.

The interaction between law and policy/practice. One cannot only look at norms form a legal perspective these days, because not all norms have yet been tested in practice and therefore require a policy assessment in order to determine their relevance, context and scope of application. That's how the Tallinn Manual started – from a question how to combine theoretical thinking of law with an emerging concern. However, the Law of Armed Conflict (LOAC), the core content of the Tallinn Manual, only covers a very small fragment of the conflict that is going on in this domain – cyber crime and clashes of national interests are not covered by LOAC.

On a high political level the discussion has moved from if international law applies to how it applies. Most legal scholars are not ready to respond to this in a balanced way, because every legal expertise cluster has a compartmentalized look at the applicability of norms – both from expertise and national implementation point of view. How a state chooses to apply the law may not be accepted on an international level. However, several cases from the past years indicate state practice on handling cyber incidents.

Estonia 2007 is a good example of how state implementation of law works in crisis: a generally accepted academic approach to privacy and data protection was overruled by national security concerns and the right and duty of the law enforcement agencies to take control over the situation. This made the Estonian Data Protection inspectorate accept an alternative interpretation of the right to privacy *ad hoc*, without much scholarly work on this and without clear exceptions to the right of privacy and personal data protection granted under international law. In 2010, the Dutch Government took action against the then largest botnet in the world and took over the botnet infrastructure to notify victims about their computers being infected. There are other practices

such as recent Microsoft cases that indicate where the limits of law are when it comes to cyber conflict resolution.

Still, how law applies is a very tricky question as international law is interpreted differently by nations and virtually all international legal instruments have a national implementation mechanism. Therefore perspectives as to what constitutes freedom of speech can differ considerably between the U.S., Europe and Asia.

There is also a historical development perspective to applying international law in cyberspace. In 1945 we did not necessarily see the international security covering non-military aspects. Today a myriad of aspects meet under the notion of 'security' and therefore often require critical review and assessment of existing interpretations. We're in a situation where we require a very clear legal answer that more than one country can actually relate to – in non-legalese. If lawyers are not able to give answers to how law applies we are soon back with the question if law applies at all. Therefore we are likely to face new proposals from countries to draft a new treaty for 'cyberspace'.

Cybercrime is a good example to look at because it's an area of law that has been developing for quite a while now. The U.S. has federal statutes dealing with computer crime and electronic evidence. Many other countries have put similar laws in place. Cyber crime is defined as crime committed against or targeting computers, or committed through use of computers or information communications technologies. So this could apply to a wide array of crime throughout the world. A computer is basically anything you can use to communicate or network with.

To combat cyber crime, three basic components are required from a legal perspective: agreement as to what constitutes substantive offences (hacking, fraud, IP, child porn, etc.); a set of investigative tools that permit obtaining of evidence (content and transactional information); and the ability to have meaningful and rapid international cooperation, both formally and informally.

As the Budapest treaty is more than a decade old, it naturally needs an update. At the same time it covers all the essential elements needed to deal with cyber crime. With political tensions topping the legal update requirements there will be a greater push for some kind of treaty at the UN level which affects ratifications of the Budapest instrument.

Internationally, however, there is an increasing recognition that cybercrime is a huge problem, and that countries must take steps to address it. So countries should put structures in place that will allow us to deal with cybercrime, and having them do so is far more important than insisting on states signing on to Cybercrime Convention.

Yet competing cyber crime initiatives are but one example of differing views on how law applies. But a similar assessment needs to be done for more or less every single norm.

We need to understand how far the international law goes and what possible national ramifications are. For instance, in the interests of national security, public safety and prevention of crime freedom of information can be limited even in Europe. The protection of speech as provided by the First Amendment to the United States Constitution is therefore not granted in that same way throughout the world.

Some frequently asked questions are, in fact, settled by state practice. Espionage by its terms violates state sovereignty. But over time, we have accepted we all do it to each other – so it's

become part of customary international law established by state practice. Espionage thus is criminalized in every domestic system but not in international treaty.

The panel concluded with some challenges that lawyers and decision-makers face when dealing with the applicability of international law.

In general it is accepted that international law applies to cyberspace just as much as elsewhere. It's a practice of ceding sovereignty to contain your opponents and to pursue national objectives.

Law, however, is never the only answer to a situation. International lawyers are focused with finding solutions to systemic problems. Foreign policy decision makers often need to focus on advancing their states' objectives. The lack of a current framework for some issues, e.g., espionage, non-state actor involvement, is partly because states want to preserve flexibility to pursue their national interests. One cannot, however, conclude that international law and national security interests are not aligned with each other. International law promotes states' own national security interests and countries often use the law to "win". All in all, law is not about being pacifist. Countries should not be shy about making legal agreements work for them.

The development of cyber conflict imposes more challenges on how we apply law. We can say with some certainty that there will be more disruptive activities in cyber space, and that the hostility level is increasing. We are dealing with a very multi-polar environment with many interested stakeholders. It is a destabilized equilibrium as everyone can have computers and decide to use them to cause harm to others. Willful misattribution makes cyberspace distinct from other areas of international engagement as there is "no badge on your police officer." Non-state actors are often outside of state control. Thus, effects-based responses are becoming the standard and this in turn complicates purely legal responses.

There have also been an increase of incidents of state acting extra-territorially apply domestic laws to protect their national interests in cyber space. Actions like this could result in a very contentious environment – a curtailing of cyber activity that is situated on someone else's territory.

Further, there are difficulties related to actually applying international law in a real-life situation – e.g. in private sector. Multinational companies struggling for compliance in international settings are caught in the crossfire.

For citation: Lotrionte and Tikk, rapporteurs, Summary for Panel 3: Applicability of International Law to Cyberspace & Characterization of Cyber Incidents. Cyber Norms Workshop 2.0, Sept., 2012. http://citizenlab.org/cybernorms2012/