EFFORTS ON HOW INTERNATIONAL LAW IS APPLICABLE IN CYBERSPACE

PETER PEDAK
MINISTRY OF FOREIGN AFFAIRS OF THE REPUBLIC OF ESTONIA

INTRODUCTION

• I was asked by the organisers to talk about the efforts on “how international law is applicable in cyberspace”.
• To begin with, I would like to explain what I mean by these terms and what I don’t.
• First, ‘international law’. In general, international law refers to legally binding norms that are embodied in numerous treaties, i.e. international agreements between states, as well as customary international law. In addition to these legally binding norms there are also many politically binding norms that guide the relations between states (e.g. most of the OSCE documents beginning with the Helsinki Final Act of 1975). However, I will concentrate my presentation on legal norms.
• The second question is what we mean by ‘cyberspace’? There is no generally recognised definition, but a version provided by the International Organisation for Standardisation can be used – cyberspace is the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. So, in short, it is a manmade environment that needs to be legally regulated as any other environment.
• Thirdly, what does ‘applicable’ mean? To put it very simply, ‘to apply the law’ means ‘to be guided by the law in your behaviour’. Sometimes one can feel a misperception that the phrase ‘international law applies’ refers only to the situation when a state has violated an obligation under international law and the victim state has taken the case to an international institution, such as the United Nations Security Council or the International Court of Justice. This is not correct. ‘Application’ does not only mean the results of a breach but also compliance. So, for instance, when a state does not carry out cyberattacks against another state, it means that it applies its obligation under the Charter of the United Nations to refrain from the use of force.
• And finally, for introduction, what is the main concern of the international community? Why is the application of international law to cyberspace so often discussed in different international fora, including our today’s workshop? The problem, as I see it, is that cyberspace is still a relatively new domain, there is not a lot of practice (including state practice), there is still not enough awareness of what the application of international law actually means and there is a natural wish to know how well international peace and stability are guaranteed. In addition to this insecurity, there are also political implications. There are old issues reappearing in the context of cyber security, e.g. the exercise of national sovereignty, the definition of armed attack or aggression, or the limits to freedom of expression. Therefore, even though cyber security has come to forefront as a predominant field of high politics, the calculus of potential solutions should never be disconnected from broader foreign, security and development policy.
UNITED NATIONS

- Coming now to the efforts that are being made to bring more clarity to the application of international law in cyberspace, who is making them and where? If we talk about the action of states and the whole new field of foreign policy called ‘cyber diplomacy’, then the most prominent forum is, of course, the United Nations.

- The discussions in the United Nations started in 1998 when Russia presented a draft resolution on developments in the field of information and telecommunications in the context of international security.

- This topic has been since then on the agenda of the First Committee of the United Nations General Assembly. The First Committee, i.e. the Disarmament and International Security Committee is one of the six so-called ‘main’ committees of the General Assembly. It deals with international peace and security. The past activities of the First Committee include international concerns of nuclear non-proliferation, chemical and biological weapons and weapons of mass destruction. Further, the disarmament of outer space has also been addressed by the First Committee, as well as issues involving regional security and terrorism.

- The General Assembly has four times mandated the Secretary General to form a group of governmental experts to report on developments in the field of information and communications in the context of international security.

- Briefly on the work of these groups (the so called GGE-s) so far: the first GGE (2004–2005) failed in the absence of critical acknowledgment and awareness of the topic and there was no final report; the second one (2009–2010) confirmed the connection between development and the use of ICTs on the one hand and international peace and security on the other; the third GGE (2012–2013) produced the current structure of dialogue (legal norms, confidence building measures and capacity building measures) + made the conclusion in its report that international law applies.

- Currently, it is the fourth time the UN GGE is gathering to discuss cyber security.

- There are 20 members in the Group. Its mandate expires this summer and hopefully a new report will be presented to the General Assembly this autumn.

HOW INTERNATIONAL LAW APPLIES TO THE USE OF ICTS BY STATES?

- The point of departure of the current GGE is the position taken by its predecessor in 2013 that ‘international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment’.

- Therefore the mandate of the Group of Governmental Experts is no longer to examine whether international law applies, but how it law applies to the use of information and communications technologies by States.

- Cyberspace has unique characteristics compared to other domains and kinetic activities. But such characteristics should not be viewed as impediments to the application of international law. Although all treaties are not explicitly adopted in response to the developments and requirements of the information age, they nevertheless govern cyberspace and State activities therein by their object and purpose. Similarly, existing norms of customary international law apply to State conduct in cyberspace.

- The GGE is focusing not on detailed interpretations of existing international law, but on making reference to some principles and instruments of international law that it deems particularly relevant for the purposes of international cyber security.
• In certain circumstances a cyber-operation might constitute use of force, act of aggression or an armed attack within the meaning of the UN Charter, but it is difficult to set concrete examples of such situations. International law is applied every day, irrespective of the lack of a clear agreement on core definitions, to terms such as sovereignty, jurisdiction, armed conflict etc. To the extent that these terms are not deemed to be necessary to be defined in general international law, we should not expect to define them in a specific context like cyberspace. The application of the concepts of sovereignty, use of force, or others can be found in the jurisprudence of the International Court of Justice.

• Since the applicability of the UN Charter has been emphasised in the 2013 report, it is important to bear in mind that the main principle is that the purposes of the UN Charter should guide State behaviour in cyberspace. Whatever we do and decide, it is important to maintain international peace and security, to develop friendly relations, and to achieve international co-operation.

• Maybe it is not a likely scenario in the nearest future that an armed conflict would be fought exclusively by cyber means. However, if there is an armed conflict ongoing and also cyber means have been used, international humanitarian law would have to be applied. It would in the interest of all states to limit humanitarian consequences of such conflict.

• Sometimes we hear arguments that the cyberspace should remain an exclusively peaceful domain and that if we confirm that international humanitarian law applies to it, it would promote its military use. To prevent conflict in cyberspace is essential, but the affirmation of the applicability of international humanitarian law would not promote conflicts but rather have a deterring effect against potential uses of ICTs in ways incompatible with international peace and security. The more it is acknowledged that there are prohibitions, the more efficient is the conflict prevention. The fact that we are not seeing cyberattacks amounting to use of force signifies that the prohibition of use of force in Article 2, paragraph 4 of the UN Charter guides state behaviour in the cyber domain. It is essential to understand that international law guides our behaviour on daily basis.

• I would also like to make a parallel showing that the development of cyber defence capabilities does not contradict the peaceful use of ICTs. Cyberspace is raising similar questions and dilemmas as the outer space raised decades ago, one of them being the discourse about peaceful use. While space and cyberspace are not necessarily comparable as domains, they both have been surrounded by political, military and technological ambitions reflecting underlying differences between countries that need to be tackled at the international level. The space law precedent of the concept of ‘peaceful use’ in international law constitutes current consensus on interpretation of this term in the context of international relations. The substance of the principle of ‘peaceful use of outer space’ has evolved to mean ‘non-aggressive use’. The same could be applied to cyberspace – it is permitted to develop cyber capabilities for defence but not for aggression.

• The GGE has also concluded in 2013 that State sovereignty and the international norms and principles that flow from it apply to States’ conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.

• The views on the exercise of state sovereignty in cyberspace are rather different. According to the strict interpretation of sovereignty, the mere “virtual presence,” regardless of damage incurred to the transgressed State’s networks, may already be seen as a breach of sovereignty. This approach may mean that there are thousands of breaches per day, thereby placing an obvious burden on the State if one would wish to
respond to all of them. It appears to be more reasonable to take the approach that sovereignty is not unlimited and not every act in cyberspace is a breach of sovereignty. One has also bear mind that the exercise of sovereignty is always balanced with the international obligations of the state concerned (such as the human rights obligations and diplomatic immunity of other states). The UN Human Rights Council adopted in July 2012 by consensus a resolution on the promotion, protection and enjoyment of human rights on the Internet, which affirmed that ‘the same rights that people have offline must also be protected online’.

- The principle of sovereignty is connected to the concept of state responsibility that covers all international obligations of States.
- In the 2013 report it was reaffirmed that “States must meet their international obligations regarding internationally wrongful acts attributable to them” and “States must not use proxies to commit internationally wrongful acts”.
- According to Article 2 of the Articles on Responsibility of States for Internationally Wrongful Acts an internationally wrongful act presupposes that there is a conduct consisting of an action or omission that: 1) is attributable to a State under international law and 2) constitutes a breach of an international obligation of the State.
- It should be borne in mind that State responsibility is not unlimited (just like I said about sovereignty). For instance, the State cannot be held responsible for the acts of its citizens if they are acting in a private capacity.
- It is true that alleged breaches of States’ international obligations related to cyberspace have not often been raised in international organisations. This does not automatically lead to the conclusion that the absence of active discussion is due to the lack of relevant norms in international law. Hesitance to bring such cases to international attention may derive from political choices and international relations in general.

WHAT NEXT? NEW NORMS

- In addition to the matters of applicability of international law, the UN GGE is also discussing the need for new political norms and confidence building measures to be evolved, but my colleague from Germany will talk more about that.
- I just limit myself to saying that international law, confidence building measures and capacity-building are complementary for the purposes of pursuing the aims of international cyber security.
- If there are proposals to elaborate new legal instruments, we should not tell what is missing before we know our shared values.
- The need for a new legal instrument could be assessed according to the following criteria: 1) What are the jointly desired and undesired outcomes associated with the issue or norm under question (why is it tabled and why is it being discussed)? The starting point for a norms discussion could be a clear understanding of the desired end state. 2) Can the desired outcomes be achieved by interpretation of existing international norms and if not, what are the gaps? 3) Are the gaps in question qualitative or quantitative and can they be overcome by procedural or substantive additions. If gaps are quantitative, are the existing instruments expandable to the required level of participation (scope of consensus) and what might be parallel implications? 4) Have new norms emerged from (state) practice and what is the consensus platform for such norms (e.g. Computer Emergency Response Teams’ cooperation)? 5) In case substantive action is required, would soft regulation be a working alternative to hard regulation?
- Instead of new legal instruments it would be wise to concentrate on the application of existing instruments. Regional cooperation is particularly important for that purpose.
• Today and tomorrow we will hear more about the criminal use of the Internet for terrorist purposes and other cybercrime.

• In these fields many regional efforts are made. For example, the Council of Europe has adopted the Convention on Cybercrime (the Budapest Convention) and the Convention for the Prevention of Terrorism. Their membership is not limited with European States. These Conventions are open for accession by all states in the world or they can at least be used as a source for inspiration.

• The same goes to numerous academic efforts made by different scholars and research institutions worldwide.

• One of the results of such academic efforts is the Tallinn Manual on the International Law Applicable to Cyber Warfare. It is written at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (that is located in my hometown). But I would like to emphasise that it is not an official document but instead an expression of opinions of a group of independent experts acting solely in their personal capacity.

• The Tallinn Manual is a reader friendly book that compiles some rules derived from existing international law and gives interpretations and examples how they could be applied. It starts by some considerations on sovereignty and jurisdiction and ends by rules applicable in armed conflict. A second edition of the Tallinn Manual, the Tallinn Manual 2.0 is under preparation and it will presumably be published next year.

• In conclusion, I believe that the questions on the application of international law to cyberspace can be solved only through examination, exchange of views and discussion, trying to find common interest. The more states and academic researchers participate in this debate, the more likely it is to find common interest and to reach consensus.