International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 6

United Nations Group of Governmental Experts: The Estonian Perspective

Marina Kaljurand

1. Introduction

The issue of cyber security did not land on the desks of politicians, lawyers and decision-makers overnight. For decades now, development and uses of information and communication technologies (ICTs) have gradually entered all areas of social and political life. Discussions of further development and use of these technologies in the context of the UN First Committee[1] – the Disarmament and International Security Committee – speak to the ICT-centricity of modern lifestyle, statehood and political affairs, and the consequent need to coordinate and concert the international community's actions for stability, security and peace in cyberspace.

Estonia is a country where ICTs are not a matter of lifestyle, but part of the society's DNA. Since the early 1990s, conscious political choices of making ICTs a driver of social and economic growth have contributed to a well-functioning information society with an effective e-government. The vulnerability of such a societal model to both mainstream and sophisticated cyber attack was acknowledged early on as an element of political priority. Cyber security and cyber defence

1 For a compiled list of documents, see United Nations Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the Context of International Security,' http://www.un.org/disarmament/topics/informationsecurity/.

are areas of Estonian national excellence which have contributed to NATO's capabilities. The 2007 test of politically contextualised cyber attacks against Estonian government web servers and public e-services confirmed that critical information infrastructure, national information systems, and online services have become potential targets, not just to criminals, but to politically and ideologically motivated state and non-state actors.

The Estonian decision to apply for the United Nations Group of Governmental Experts on the Developments in the Field of Information and Telecommunication in the Context of International Security (UN GGE) membership in 2008 was therefore a reflection of our commitment to upgrading our ICT-centric lifestyle and statecraft to a new level of security and confidence, going beyond fragmented solutions and implementing not just nation-wide, but internationally shared practices and norms for keeping cyberspace open, resilient, peaceful and secure.

For Estonia, as for any country, 'cyber' is not an isolated issue. ICTs serve as drivers and enablers for any area of business and politics. Our success in implementing a functional and efficient information society on the premises of the free flow of information, public-private-coordinated architecture, and a culture of responsibility requires us to leverage the UN GGE to further our understanding, practice and mentality with the help of other countries, both with similar and deviating views and experience. By actively contributing to international cyber diplomacy, Estonia seeks to maintain and further develop its reputation and expertise in building a safe cyberspace for all.

For Estonia, participation in the UN GGE has been an essential foreign policy goal that is in line with our national ICT policy. Technology-dependence and cyber attacks are the new normal and it is paramount for ICT-savvy countries to coordinate their contributions to the security of our common information infrastructure.

This chapter will focus on the Estonian perspective on the UN GGE as one of the few global forums for high-level discussions on cyber norms. Drawing on previous experience, the chapter will explain Estonian positions and views on the main topics addressed in the Group's discussions.

2. The Mandate and the Membership of the 2014/2015 UN GGE

The 2013 UN GGE, building on the 2010 report, concluded with a tripartite agenda. On the issue of international law, the consensus on the applicability of international law to cyber security was accompanied by a recommendation to further study and develop common understandings of how such norms shall apply to state behaviour

and the use of ICTs by states. The experts also noted that 'given the unique attributes of ICTs, additional norms could be developed over time'.[2] The group also set the stage for further discussion of confidence-building measures in the context of international cyber security. The agenda of capacity-building was to be guided by an earlier UN General Assembly Resolution 64/211 on the creation of a global culture of cyber security.[3]

All these themes were furthered during the 2014/2015 negotiations, as mandated by the UN Secretary-General. In addition, a separate agenda of norms of responsible state behaviour branched out of the international norms and principles dialogue.

The mandate of the 2014/15 UN GGE was to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules and principles of responsible behaviour of states and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by states, as well as the concepts aimed at strengthening the security of global information and telecommunications systems.[4]

In 2014, the group was increased to 20 experts from the previous 15 to be geographically and politically more balanced in the discussions of an increasingly urgent and controversial set of issues. Interest towards the agenda and activities of the UN GGE has steadily grown alongside with the increased number and sophistication of cyber threats and attacks. The principle of equitable geographical distribution brought in experts from Africa and Latin America, leaving out Australia, the chair of the 2012/2013 UN GGE, and Canada.

2 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, para. 16 (24 June 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

3 Ibid, para. 32.

4 United Nations, General Assembly resolution 68/243, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/68/243, para. 4 (9 January 2014), http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2014-2015-a-res-68-243-eng-0-589.pdf.

Table 1. Membership of the UN GGE.

Country	2004-2005[1]	2009-2010[2]	2012-2013[3]	2014-2015[4]
Argentina			X	
Australia			X*	
Belarus	X	X	X	X
Brazil	X	X		X*
Canada			X	X
China	X	X	X	X
Colombia				X
Egypt			X	X
Estonia		X	X	X
France	X	X	X	X
Germany	X	X	X	X
Ghana				X
India	X	X	X	
Indonesia			X	
Israel		X		X
Italy		X		
Japan			X	X
Jordan	X			
Kenya				X
Malaysia	X			X
Mali	X			
Mexico	X			X
Pakistan				X
Qatar		X		
Russia	X*	X*	X	X
South Africa	X	X		
South Korea	X	X		
Spain				X
UK	X	X	X	X
US	X	X	X	X

**Chair of the Group*

3. Estonia's Main Considerations in the 2014/2015 UN GGE

It was the third time that Estonia had been selected as a member of the UN GGE. Therefore, our self-evident point of departure was that the Group should build on its work in the previous reports and not lose sight of the progress already achieved.

In comparison with the 2010 report, the most significant achievement of the 2012/2013 UN GGE was reaching a consensus that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. After this general affirmation, the Group was expected to analyse further the application of international law, both of peacetime norms and international humanitarian law in the context of use of ICTs that relate to national and international peace and security. In doing so, it was important to keep in mind that

international law relevant to the use of ICTs by states resides in numerous treaties, which, albeit not explicitly adopted in response to the developments and requirements of the information age, 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. 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.

In setting our goals for the work of the 2014/2015 UN GGE on international law, Estonia took a reasonably pragmatic approach. A major breakthrough on detailed interpretations of international law applicable in cyberspace was not to be expected. However, any consideration that the Group would be able to bring out and agree upon, in addition to the general declaration of 2013, would be a positive development. Estonia recognised that there are complex issues concerning the application of international law, in particular the 'thresholds' for a breach of sovereignty, use of force, aggression or armed attack. However, in our view such questions cannot be set theoretically, but rather on a case-by-case basis and taking into account all relevant facts and circumstances. The absence of definitions of these concepts does not mean the impossibility of application of international law. International law is applied every day, irrespective of the lack of clear agreement on core definitions of terms such as sovereignty, jurisdiction, and armed conflict. To the extent that it is not deemed necessary that these terms are defined in general international law, we should not expect to define them in a specific context like cyberspace. Neither should we undermine the authority of existing international law by giving detailed interpretations. We should rather make reference to the principles and instruments of international law that the UN GGE deems particularly relevant for the purposes of international cyber security. Estonia also believes that these efforts of the UN GGE should be complementary with the ongoing work addressing other issues, such as cyber crime, cyber terrorism, human rights, and Internet governance, by other international organisations and forums.

Estonia urged the UN GGE members and other states, individually and cooperatively, to study, analyse and discuss how international law is to be applied with the help of different academic groups in order to ascertain diverse expert views on the matter.

Another major contribution of the 2013 UN GGE, besides the confirmation of the applicability of international law, was the inclusion of confidence-building measures in its report. In continuing the elaboration of these measures it was important to keep in mind that the approach to international cyber security should be holistic. For Estonia, norms (both legally and non-legally binding), confidence-building measures, and measures for capacity-building are complementary.

4. Estonian Proposals for Norms of Responsible State Behaviour

After the first meeting in July 2014 all members of the Group were invited by the chair to present their position papers in order to gather food for thought and discussion. Estonia took a very pragmatic and practical approach and submitted its proposals in September 2014. Without prejudice to the importance of the application of international law, Estonia decided to focus on some proposals for norms of responsible state behaviour. In later discussions and in the final report, these norms were to be characterised as voluntary and non-legally binding.

The topics highlighted by Estonia were chosen on the basis of our own practical experience, and in particular the lessons learned after the cyber attacks in 2007. We kept also in mind that these proposals might have potential for consensus since they should reflect common interests of all states to ensure the safety of their information and communication systems. Also, it was expected that there would be more divergent views on the details of the application of international law.

The suggestions made by Estonia concerned: 1) protection of critical (financial) infrastructure; 2) cooperation in incident response; and 3) mutual assistance in resolving cyber crises. In addition to these norms Estonia also presented its views on capacity-building.

4.1 Protection of Critical Infrastructure

Estonia is of the opinion that the protection of ICT-based or ICT-dependent critical infrastructure subject to a state's jurisdiction constitutes responsible state behaviour. Our understanding of critical infrastructure is based on UN General Assembly Resolution 58/199 ('Creation of a global culture of cyber security and the protection of critical information infrastructures').[5] The key measures to be taken in this regard stem from the UN General Assembly Resolution 64/211 ('Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures').[6]

The preamble of Resolution 58/199 sets a non-exhaustive list of examples of critical infrastructures, such as those used for the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health – and the critical information infrastructures that increasingly interconnect and affect their operations. In the spirit of the Resolution, states are encouraged to define their nationally

5 United Nations, General Assembly resolution 58/199, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures,* A/RES/58/199 (30 January 2004), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

6 United Nations, General Assembly resolution, *Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures*, A/RES/64/211 (17 March 2010), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211.

critical infrastructure, assign responsible institutions, and develop protection measures including comprehensive national crisis preparedness and response procedures. States are expected to facilitate cross-border cooperation to address vulnerabilities of critical information infrastructure transcending national borders.

Thus, it was our aim that the UN GGE could call upon states to protect their critical infrastructures (within their own territories and at their own responsibility) and to cooperate in this field as much as possible. How exactly this will be done, remains to be decided by the state itself.

It is incumbent upon each state to take action to ensure that its information systems are reliable and as safe as possible from malicious uses. The UN GGE can encourage states to take the national steps necessary to ensure the integrity of their domestic critical infrastructure. The UN GGE should also emphasise the interconnected nature of national critical infrastructures.

Later during the deliberations arguments were raised that the publication of the list of critical infrastructures would make them more vulnerable to attack. Estonia agrees that it is up to each state to decide whether to make the list of its critical infrastructure public or not. However, in our opinion the publication of the list would not make it more vulnerable to attack, but would increase confidence and clarity between states. Of course, the detailed information on the use of the infrastructures would remain classified.

Although the identification of critical infrastructures remains to be decided by each state itself, it is useful to bear in mind that there still exists a certain hierarchy between different types of infrastructure. Some of them, such as energy and telecommunication infrastructures, form the basis for the proper functioning of others. According to Estonian experience, critical infrastructures may be additionally categorised at a national level and be subject to different levels of security requirements and priorities.

While we consider it necessary to continue developing practices on the protection of all types of critical infrastructure, we proposed to focus particularly on the issue of stability and security of the financial system, which we consider to be in the interest of all states due to its centrality for the functioning of individual economies as well as the global economy as a whole. Due to interdependencies, attacks against individual financial institutions as well as financial services can cause extensive damage and reduce public trust toward the digital economy.

The UN GGE concluded its report with a number of recommendations concerning the protection of critical infrastructure, both in the section on norms, rules and principles for the responsible state behaviour,[7] as well as on confidence-building measures,[8] and on capacity-building.[9]

7 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* A/70/174 (22 July 2015), para. 13; sub-para. (f), (g), (h), (j), http://www.un.org/ga/search/view_doc.asp?symbol=A%2F70%2F174&Submit=Search&Lang=E.

8 Ibid, para. 16, 17; sub-para. (a), (c), (d).

9 Ibid, para. 21; sub-para. (b) and (e).

4.2 Cooperation in Incident Response

Cooperation between national institutions with computer incident response responsibilities, such as Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Team (CSIRTs), is one of the most important preconditions for preventing as well as solving both domestic and international cyber incidents.

In the 2013 UN GGE report it was agreed that States should consider the development of practical confidence-building measures, including exchanges of information and communication between national CERTs bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels.

Estonia proposed to bring this further by declaring that a state should not knowingly support acts intended to prevent a national CERT or CSIRT from cyber incident response. Also, the CERTs and CSIRTs should be provided with a sufficient number of multilateral formats for regular meetings. Participation in working group meetings at technical level helps to build confidence. One should avoid isolation on the basis of national security interests and understand that cyber security is transnational.

This would not necessarily entail the adoption of new legal instruments. The UN GGE should not promote further international regulation where commonly agreed goals can be achieved and state practices have emerged on the basis of existing international law. States have developed commendable practice in CERT cooperation, such as information exchange about vulnerabilities, attack patterns, and best practices for mitigating attacks. Estonia invited the UN GGE to support this practice and encourage its expansion. This includes supporting the handling of ICT-related incidents, coordinating responses, and enhancing regional and sector-based cooperation practices.

The issue of CERTs was reflected in the final report in the norms' section,[10] as well as in the confidence-building measures[11] and capacity-building[12] sections.

4.3 Mutual Assistance in Resolving Cyber Crises

The issue of mutual assistance in resolving cyber crises is closely connected to cooperation between CERTs. Considering the cross-border nature of cyber threats, states should assist other states in resolving cyber crises, particularly by mitigating on-going incidents. This would build confidence that cyber crises will not be unnecessarily escalated, as well as an expectation of reciprocation in the future.

Estonia suggested that the Group should consider types of assistance to be expected and provided. Further mechanisms include creating procedures for expedited assistance, organising relevant national and regional exercises to enhance preparedness for handling real incidents, and promoting relevant implementation practices of existing multi- and bilateral agreements.

10 United Nations, General Assembly, *Group of Governmental Experts*, A/70/174, para. 13; sub-para. (k).
11 Ibid, para.17; sub-para. (c) and (d).
12 Ibid, para. 21; sub-para. (a).

4.4 Capacity-Building

Enhanced capacity-building and awareness-raising in cyber security helps to improve means and methods to counter cyber threats. We deem it necessary to provide assistance and cooperation to technologically less developed countries in order to enhance their cyber security capabilities. Estonia is prepared to contribute to relevant programs and activities, including risk analysis, training, education, information exchange, and research and development.

5. Main Issues on the Application of International Law Discussed by the UN GGE

Although in its position paper Estonia concentrated on a set of norms of responsible state behaviour, we were equally prepared that the main discussions in the Group would be focused on the application of international law.

5.1 Military Use of Cyberspace, Right to Self-Defence and International Humanitarian Law

There were divergent views expressed in the Group whether cyberspace should remain an exclusively non-military domain, and whether any reference in its report to humanitarian law would instigate military conflict.

Estonia agrees that an armed conflict fought exclusively by cyber means might not be the most urgent topic for the UN GGE as there are other more pressing issues to tackle. For example, according to our assessment, the most harmful cyber attacks are potentially those that may fall below the 'use of force' threshold but still target a nation's critical infrastructure and associated information systems. Failures of, or disruptions to, critical information systems may impact extensively upon the normal functioning of society with potentially disastrous consequences.

This being said, it is important to stress that the development of cyber defence capabilities does not contradict the peaceful use of ICTs. If there is an armed conflict ongoing and also cyber means have been used, international humanitarian law would have to be applied. It would be in the interests of all states to limit the humanitarian consequences of such conflict. 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 deterrent effect against potential uses of ICT in ways incompatible with international peace and security. The more it is acknowledged that there are prohibitions, the more efficient is the conflict prevention. One could argue that the fact that we are not seeing cyber attacks

amounting to use of force signifies that the prohibition of use of force in Article 2, paragraph 4 of the UN Charter guides states' behaviour in the cyber domain.

I would also like to make a reference to a comparable debate in the history of international law and relations. Cyberspace is reinforcing similar questions and dilemmas to those raised by the use of outer space 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.[13] 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 taken into account in the discussions regarding cyberspace.

Those members of the Group who spoke in favour of cyberspace as a non-military domain opposed also any reference to states' right of self-defence or the application of international humanitarian law. Having understanding for these different views, Estonia nevertheless believed that agreement should be possible and made efforts to help to reach consensus, which eventually was reflected in the report as follows:

> 'Underscoring the international community's aspirations to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter of the United Nations applies in its entirety, the Group noted the inherent right of states to take measures consistent with international law and as recognised in the UN Charter. The Group recognised the need for further study on this matter.'

The report does not explicitly mention the right of self-defence or the applicability of Article 51 of the UN Charter. However, it is clear that the notion 'inherent right' makes reference to the right to self-defence within the meaning of Article 51. The report also makes note of the principles of humanity, necessity, proportionality, and distinction, thus clearly speaking to the applicability of international humanitarian law. At the same time one should not forget the other part of the compromise ('the Group recognised the need for further study on this matter') which means that the discussions might continue in the next UN GGE.

5.2 Sovereignty and Due Diligence

One of the most controversial issues discussed in the UN GGE concerned the limits of state sovereignty and ultimately what would be considered as a breach of sovereignty. In 2013 the UN GGE concluded that state sovereignty and the international norms and principles that flow from it apply to states' conduct of ICT-related

13 See also Paul Meyer's comparison of outer space and cyberspace norms in chapter 8.

activities and to their jurisdiction over ICT infrastructure within their territory. More or less the same was reiterated in the 2015 report.

The views on the exercise of state sovereignty in cyberspace remain 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.

Estonia believes that one should rather take a reasonable approach that sovereignty is not unlimited. Also the UN GGE could not agree on any specific threshold of what would constitute a breach of sovereignty. In the next UN GGE it would be worth trying to discuss some phenomena that would indisputably constitute a breach of sovereignty, although there could never be an exhaustive list of them.

One specific aspect connected to the sovereignty is the concept of due diligence, i.e. the principle formulated by the International Court of Justice in the *Corfu Channel* case[14] that every state has an obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states. The Group could not agree that there exists such an obligation with regard to cyberspace under international law, although one could draw parallels with the findings of the International Court of Justice in *Corfu Channel*. Without prejudice to the possible future extension of the principle of due diligence to cyberspace, the 2015 Report reflects it in the section of non-legally binding norms of responsible state behaviour: 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs'. As such, states acknowledge the need for respecting the principle of due diligence with regard to cyberspace, but it remains unconfirmed whether it is a legal obligation or not.

5.3 Cyber Terrorism

Some members of the Group were willing to include in the report detailed aspects on the fight against cyber terrorism. For others, it raised serious doubts both because of the mandate of the UN GGE and the vagueness of the notion of terrorism, and even more so of cyber terrorism. It also appeared that the proposals were not to address at first hand terrorism itself, but rather activities that support it like incitement to, financing of, and training for terrorism, as well as the recruitment of terrorists. One should recall that these acts are not terrorist offences *per se* (i.e. within the classical meaning of acts of violence), but are acts that might lead to the commission of a terrorist offence. In criminalising these preparatory acts one should pay special attention to the need to find the proper balance between the prevention of crimes and the protection of human rights.

Nonetheless, Estonia believes the UN GGE should not go into further details on terrorism. The UN's action to counter terrorism has been mainly coordinated by

14 The Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania), 4 Reports of Judgments (International Court of Justice 1949).

the Sixth Committee (Legal Committee).[15] Negotiations on a draft Comprehensive Convention against International Terrorism have been underway in the Ad Hoc Committee established by the General Assembly since 1996.[16] The Ad Hoc Committee did not meet in 2014, since more time was required to achieve substantive progress on the outstanding issues. It was our firm belief that our Group should not duplicate the work of the Ad Hoc Committee.

One should also not forget regional work already done. There are currently 40 instruments – 18 universal (14 instruments and 4 recent amendments) and 22 regional – pertaining to the subject of international terrorism.[17] The Council of Europe has examined the notion of cyber terrorism and the potential need for a new treaty since 2006. Its Committee of Experts on Terrorism (CODEXTER) found in 2007 that the primary focus should be on ensuring the effective implementation of the existing conventions, as new negotiations might jeopardise their increasing impact on the international fight against cyber crime and terrorism. There are two main conventions of the Council of Europe dealing with, *inter alia*, cyber terrorism: the Convention on Cybercrime (2001)[18] and the Convention on the Prevention of Terrorism (2005).[19] Both are open to all states for accession. The effective implementation of the Cybercrime Convention would ensure that national legislations provide appropriate sanctions for cases involving serious attacks, including terrorist ones, on IT-based or IT-general infrastructure. The Convention on the Prevention of Terrorism targets the dissemination of illegal terrorist content on the Internet, as well as training for terrorism and recruitment of terrorists.

Likewise, one should bear in mind the existing UN Security Council Resolutions related to the use of ICTs for terrorist purposes, in particular Resolution 1624 (2005).[20] It 'calls upon all States to adopt such measures as may be necessary and appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts'. That includes incitement by the use of ICTs and gives a solid basis for the prevention of terrorism.

All in all, we acknowledge that terrorism is a threat to international and national security and that terrorists use also ICT to achieve their aims. However, there are already a number of universal and regional instruments on the fight against terrorism whose effective implementation would also target cyber terrorism.

15 For more, see United Nations, 'General Assembly of the United Nations Legal – Sixth Committee,' http://www.un.org/en/ga/sixth/.

16 For more, see United Nations, 'Measures to Eliminate International Terrorism. Ad Hoc Committee Established by United Nations, General Assembly resolution 51/210 of 17 December 1996,' http://www.un.org/law/terrorism/.

17 See the latest report by the United Nations Secretary General: United Nations, General Assembly, *Measures to Eliminate International Terrorism: report of the Secretary-General*, A/67/162 (19 July 2012), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/67/162.

18 *Convention on Cybercrime*, Budapest, 23 November 2001, *Council of Europe Treaty Series*, No. 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

19 *Council of Europe Convention on the Prevention of Terrorism*, Warsaw, 16 May 2005, *Council of Europe Treaty Series*, No. 196, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008371c.

20 Security Council resolution 1624, *Resolution 1624 (2005)*, S/RES/1624 (14 September 2005), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/510/52/PDF/N0551052.pdf?OpenElement.

5.4 Human Rights

Much for similar reasons as for terrorism, the details of the application of human rights do not fall within the competence of the First Committee. Their insertion into the report is necessary to balance the emphasis on state sovereignty and to make sure that the exercise of sovereignty is not without limits and that a state must respect its other international obligations, including human rights obligations.

Estonia was a member of the UN Human Rights Council when it 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'.[21] A reference to that Resolution was also included in the UN GGE report.[22] As a balancing compromise General Assembly Resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age) were also referred to.[23]

5.5 Possible New Instruments?

Since the beginning of the process of discussions in the UN on international cyber security proposals have been made to start negotiations for a new instrument. One of such proposals is the draft Code of Conduct submitted by China, the Russian Federation and some other countries. Partly the draft reflects existing international law (e.g. 'To comply with the Charter of the United Nations and universally recognised norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms').[24] In other parts it includes concepts that do not reflect the existing law and raise doubts of their objectives ('… respect for the diversity of history, culture and social systems of all countries; to prevent other States from exploiting their dominant position in information and communications technologies' etc.) It could certainly add impetus to the debates in the next possible UN GGE, but starting negotiations on the draft Code of Conduct for its adoption by the UN GA would be premature.

On a more general note, we should not confirm what is missing before we have concluded serious analysis. Estonia does not preclude the need for new norms to be elaborated over time, but this need for a new (legal) instrument should be assessed according to the following criteria:

21 United Nations, General Assembly resolution 20/8, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/RES/20/8 (6 July 2012), http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

22 United Nations, General Assembly, *Group of Governmental Experts*, A/70/174, para. 13; sub-para. (e).

23 United Nations, General Assembly resolution 68/167, *The Right to Privacy in the Digital Age*, A/RES/68/167 (21 January 2014), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167; United Nations, General Assembly resolution 69/166, *The Right to Privacy in the Digital Age,* A/RES/69/166 (10 February 2015), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166.

24 United Nations, General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/69/723 (13 January 2015), https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

- 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.
- Can the desired outcomes be achieved by interpretation of existing international norms, and if not, what are the gaps?
- Are the gaps in question qualitative or quantitative (i.e. an insufficient number of parties), 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 the parallel implications?
- Have new norms emerged from (state) practice and what is the consensus platform for such norms (e.g. CERT cooperation)?
- If substantive action is required, would politically binding norms be a working alternative to legally binding norms?

We admit 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. Hesitation in bringing such cases to international attention may derive from political choices and international relations in general.

6. Conclusions on the 2015 Report

Estonia sees the 2015 Report as a remarkable achievement. Given the ideological battle and differences in national ICT capabilities, taking the 2013 consensus further was a difficult, but successfully completed task. In particular, Estonia welcomes attention to norms of responsible state behaviour that, in the absence of shared detailed consensus on how international law applies in cyberspace, is a way forward towards building such understanding.

Friedrich Fromhold Martens, a renowned jurist of Estonian origin, attending the Hague Peace Conferences in late 19th century, faced in many ways a similar question to that which the UN GGE and the international community are facing today. At the time, legal rules of land warfare were in debate and raised different reactions from different countries. The Martens clause which appeared in the Convention with respect to the laws of war on land (Hague II, 29 July 1899),[25] stated that:

25 First included in the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land. *Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*, The Hague, 29 July 1899, https://www.icrc.org/ihl/INTRO/150?OpenDocument.

> 'until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilised nations, from the laws of humanity and the requirements of the public conscience.'

In the spirit of the Martens clause, it is Estonian reading of the conclusion that international law is applicable in the context of cyber security, and that countries want to remain bound by the letter and disposition of international law. Estonia regards the commitment to discussing norms of responsible state behaviour as a very useful method for both reflecting on different national views on the applicability (limits and contents) of international law as well as an indication as to where additional normative clarity might be needed and developed over time.

Estonia welcomes additional emphasis on the issue of confidence-building, a concept that the OSCE countries have been able to put into practice after agreeing to a set of initial measures in December 2013.[26]

Capacity-building has always been close to Estonian interests and priorities, and there are several ways in which Estonia can contribute to implementing the guidance of the UN GGE. In particular, Estonia is willing to contribute to better awareness and implementation of international law. We are also working with several countries to promote and broaden our experience with ICTs as the engine of social and political affairs. E-governance and e-democracy are horizontal priorities of Estonian development cooperation.

7. The Way Forward

There are arguments for and against continuing the UN GGE discussions in 2016. On the one hand, there is increasing interest among the international community towards the issue of international cyber security, and a willingness to develop shared understanding on threats and their mitigation. Cyber threats and advanced uses of ICTs in general have become the normal, inviting national strategies on responsible development and use of these technologies. On the other hand, there are limits to what the UN GGE can achieve at a practical, applied level; with the experts continuing high-level discussions about the uses of ICTs, these discussions might benefit from the implementation of the existing UN GGE guidance at national level

26 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,' PC.DEC/1106 (Organization for Security and Co-operation in Europe, Permanent Council, 975th Plenary Meeting, 3 December 2013), http://www.osce.org/pc/109168?download=true.

and socialisation of the lead items in other international and regional organisations. There is also a real risk of not being able to cover significant new ground immediately, both due to remaining differences on some of the key items and in the absence of practice-based feedback.

Estonia supports the continuation of the work of experts in the UN GGE format. In our view the group has been able to considerably deepen understanding, if not appreciation, of different national and expert views on international cyber security. Given its mandate, the UN GGE is unique and remains one of the very few forums for developing relevant views globally.

The UN GGE has been criticised for is exclusivity; the first Group featured 15 members and in 2014 the Group was extended to 20. Such criticism, however, would need to take into account the uniqueness of the UN GGE format in the first place; it is not intended to replace UN decision-making processes or to assimilate expert conferences on the subject. The task of the UN GGE is to allow experts to inform the UN Secretary-General of acute issues and possible solutions, and thus it would not be practical to extend the Group. The question instead becomes whether, given the increasing expert and political interest towards the issue, other forums and processes could be used to take all or parts of the agenda forward.

Since 2009, the format has proven a useful and efficient mechanism for deepening common understanding about ICT-related threats to international peace and security, and mitigations against such threats. We have approximated our views on threats, committed to cooperation, and pledged to stay bound by the existing international law, in particular to the UN Charter and to international humanitarian law. We have applied the concept of confidence-building measures and are discussing norms of responsible state behaviour in cyberspace, a relatively new concept in international policy. Estonia is committed to contributing to the next UN GGEs as well as to other international forums and processes that seek to achieve the goal of an open, resilient, secure and peaceful cyberspace.

Having been a member of the UN GGE since 2009, Estonia seeks alternative paths for better inclusion of a variety of views in the Group's discussions. In particular, Estonia has invited and will keep inviting dialogue among the Nordic and Baltic countries, with the view of bringing to the GGE discussions views beyond its national emphasis and focus. Estonia is also looking to develop capacity-building programmes that would allow dissemination of the Estonian experience and observations about the matters considered by the UN GGE among countries that want to carry out democratic reforms using ICT and want to learn from our experience, such as Ukraine, Georgia, Moldova, Afghanistan, Tunisia, the Palestinian Authority and others.

Between the GGEs, the Estonian emphasis is on implementation of the guidance and experience obtained during the process and enshrined in the Report. Estonia's goal is to assume more individual and better collective responsibility for the security and defence of its ICT infrastructure and national IT systems and services. In doing

this, Estonia seeks partnership with countries that can help us to achieve this goal by example, shared values and interests, integrated infrastructure, or critical review. We are open to processes and platforms that help both implement and augment the agenda of the UN GGE and international cyber security more broadly. We are ready and willing to cooperate even more closely with the private sector, academia and civil society because only through inclusiveness and cooperation can we be successful in developing a stable, open, secure, resilient and peaceful cyberspace nationally, regionally and globally.[27]

27 The author wants to thank the experts from the Ministry of Foreign Affairs, the Ministry of Defence, the Information System Authority, Tartu University, the NATO Cooperative Cyber Defence Centre of Excellence and the Cyber Policy Institute for their professionalism, commitment and excellent expertise. It was noted and highly appreciated.