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

CHAPTER 1

Introduction

Anna-Maria Osula and Henry Rõigas

1. International Norms Limiting State Activities in Cyberspace

Cyberspace has created both great opportunities for, and serious threats to, states and non-state actors. This has led to a common understanding that behaviour pertaining to the use of information and communication technologies (ICTs) has to be limited in order to prevent conflicts that endanger international peace and security. Although these concerns also apply to other subjects, the focus of the current discussions in the context of international security remains primarily on restraining the activities of states as the most capable actors.

Recent cyber security related discussions in international forums indicate 'cyber norms' or cyber 'norms of behaviour' as the most suitable vehicles for guiding states' behaviour in cyberspace. The main goals for agreeing on norms are believed to include increased predictability, trust and stability in the use of ICTs, hopefully steering states clear of possible conflict due to misunderstandings. Additionally, norms are seen as guiding principles for shaping domestic and foreign policy as well as a basis for forging international partnerships.

However, despite being frequently addressed by policy-makers, academia, non-profit organisations and the private sector, it is often unclear what is meant by the very concept of a 'norm'. Indeed, a closer look at different actors and venues reveals that various platforms promote different types of norms – for instance, of a legal, political, technical or moral nature – but it is often not evident (sometimes, it seems, even to the discussing parties) which types of norms are the focus of the debate.

Inevitably, this lack of a common conceptualisation of a 'cyber norm' results in difficulties in reaching a consensus on the accompanying policy discourse.

The book *International Cyber Norms: Legal, Policy & Industry Perspectives* is a result of a series of workshops organised by the NATO CCD COE during 2014-2015.[1] The aim of the collection of articles is to shed light on the different approaches to 'cyber norms' in various research domains. The articles outline how different disciplines define, prioritise and promote norms, and suggest approaches for developing cyber norms. We hope that the specific angles from which our distinguished authors tackle cyber norms will benefit the research community as well as explain the difficulties related to agreeing on common cyber norms.

As our book focuses mainly on international cyber norms that aim to regulate malicious or potentially harmful cyber activities between states, this introductory article paves the way for the following chapters of the book by giving an overview of the main international platforms where the most advanced cyber powers have addressed the subject.

Amongst the various alternatives that can be applied, we refer to Finnemore and Sikkink's approach of defining a 'norm' as 'a standard of appropriate behaviour for actors with a given identity'.[2] This broad definition implies that norms can at the same time substantially differ in scope and legal 'bindingness', as well as featuring legal, political, technological, ethical, or social characteristics. In the context of the international discussions covered in this introduction, we differentiate between two principal types of norms that regulate state activities in cyberspace. These are:

(1) International norms that carry a legally binding obligation (i.e. treaties and other sources of international law);[3] and
(2) International norms that act as points of reference for expected behaviour but are not subject to legal enforcement mechanisms (e.g. legally non-binding voluntary norms of behaviour) and are usually expressed in diplomatic agreements.[4]

[1] The NATO CCD COE has brought together representatives from academia, private sector and government to discuss cyber norms in three iterations. The first workshop was held in cooperation with Professor Paul Cornish in Stockholm in April 2014 (https://ccdcoe.org/cyber-norms-international-relations.html); the following workshops were held as part of NATO CCD COE's annual CyCon conference, in cooperation with the Estonian Ministry of Foreign Affairs, in 2014 and 2015 (https://ccdcoe.org/cycon/past-cycon-conferences.html).

[2] Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change,' *International Organization* 52 (1998): 887-917.

[3] According to Article 38 (1) in the Statute of the International Court of Justice (ICJ), sources of international law are (a) international conventions, (b) international customs, (c) general principles of law, and (d) judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law. See United Nations, *Charter of the United Nations* and *Statute of the International Court of Justice* (24 October 1945), 1 UNTS XVI, http://www.icj-cij.org/documents/?p1=4&p2=2#CHAPTER_II.

[4] Many also apply the terms 'hard' and 'soft' law in this context, see, for example, Dinah Shelton, 'Normative Hierarchy in International Law,' *The American Journal of International Law* 100 (2006): 291-323. Furthermore, we highlight that this dichotomy is a simplification used for explanatory purposes as Jan Klabbers puts it: 'law is not (or should not be) an on/off, binary phenomenon, but rather a mode of analysis which can account for various shades of grey. … Actions can be more or less legal or illegal; and agreements can be more or less binding and non-binding.' See more in Jan Klabbers, *The Concept of Treaty in International Law* (The Hague: Kluwer, 1996), 157.

Accordingly, after a great degree of generalisation, we apply the terms '*legal norm/legally binding norm*' and '*political norm/politically binding norm*' in this introduction.[5] As presented in greater detail in later chapters of this book, especially in the context of cyber security, we can see these two types of norms intertwining and overlapping which adds complexity to the discussions in the different forums mentioned below. The following overview will further show that cyber norms are being discussed not only on global and multilateral levels,[6] but also bilaterally and in forums involving non-state stakeholders.

2. Global perspective

2.1 United Nations Group of Governmental Experts

As the main global forum for states to discuss and agree upon issues regarding international security, the United Nations (UN) has been one of the main venues to address issues of international cyber security.[7] In the context of cyber norms, the UN Group of Governmental Experts (UN GGE) is the best-known platform for states to discuss national positions on matters related to developments in the field of ICTs.

These discussions are held under the auspices of the First Committee among a group of nations that is formed on the basis of equitable geographical distribution.[8] This process has been ongoing since 1998, but constructive collaboration between states has, from the beginning, been challenged by different approaches regarding terminology, the scope of the problem, the mandate and role of the UN, and perspectives on the threat.[9]

As a significant development, the UN GGE reached a 'landmark consensus'[10] in 2013 when 15 countries agreed that 'international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability

[5] As an expression of the complexity of this research area, we acknowledge that the definitions provided by the authors in the book can differ from the approach applied in this introductory chapter.

[6] For an overview of legal and policy developments in the most prominent international organisations active in cyber security, see NATO CCD COE's 'INCYDER' database, https://ccdcoe.org/incyder.html.

[7] To read more on cyber norm emergence in the UN, see Tim Maurer, 'Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-Security,' Discussion Paper 2011-11, *Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School* (2011), http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

[8] The First Committee is also known as the Committee on Disarmament and International Security that is one of the six main committees working on a multiple of issues relevant for the United Nations General Assembly (UNGA). See more in 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/.

[9] Read more on the historical development of these challenges in Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunications in the Context of International Security: Work of UN First Committee 1998-2012* (Geneva: ICT4Peace, 2012), https://citizenlab.org/wp-content/uploads/2012/08/UN-GGE-Brief-2012.pdf.

[10] Jen Spaki, US Department of State, *Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues*, 7 June 2013, http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

and promoting an open, secure, peaceful and accessible ICT environment'.[11] This consensus, reiterated by the global community many times since, is an essential first step in understanding contemporary discussions on cyber norms. The agreement indicates a popular view of many states and other stakeholders, who see existing international law such as the UN Charter or the laws of armed conflict as the main source for regulating offensive state behaviour in cyberspace. The core problem here is that there is no clear understanding of, or agreement on, how these legal norms apply to the complex area of cyberspace.[12]

While the consensus on the applicability of international law expressed in the 2013 report strongly suggests that further discussions should primarily focus on how the existing law applies, the report also draws attention to the 'unique attributes' of cyberspace and notes that new norms could be developed over time.[13] Indeed, there have been critical remarks questioning whether existing international law can effectively govern state activities in cyberspace, given the nature of the most prominent cyber incidents such as the Sony attacks or the widely reported cyber espionage campaigns.[14] As a possible solution, some states view the discussions at the UN GGE as the best means by which to establish a common understanding regarding additional politically binding norms of behaviour and 'do not believe that attempts to conclude comprehensive multilateral treaties or similar instruments would make a positive contribution to enhanced international cyber security at present'.[15] To help understand the role of existing public international law, chapters 2, 3 and 4 explain the nature of legal norms and focus on how these norms could be applied to state activities in cyberspace.

The UN GGE reports are also a good example of the somewhat confusing terminology often used in discussions on cyber norms. For instance, in the 2013 report, one may notice a puzzling use of language that makes recommendations on 'norms, rules and principles of responsible behaviour by States' without distinguishing between the three. Later in the text, 'norms and principles' are sometimes used together, but 'rules' are never separately mentioned, thus bringing into question their role in the whole report altogether. Furthermore, throughout the report it remains unsettled whether the 'norms' discussed are legally or politically binding. Use of phrases like 'norms derived from existing international law'[16] would suggest that the norms under scrutiny refer to 'international legal norms' that have a legally binding nature. However, the same 'norms' seem also to refer to a number

[11] 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 (24 June 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[12] See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013). 'Tallinn Manual 2.0', focusing on cyber operations conducted during peacetime, will be published in the end of 2016. Read more on the Tallinn Manual process, hosted by the NATO CCD COE, here: https://ccdcoe.org/research.html.

[13] United Nations, General Assembly, *Group of Governmental Experts*, A/68/98.

[14] David Fidler, 'The UN GGE on Cybersecurity: How International Law Applies to Cyberspace,' *Council on Foreign Relations, Net Politics Blog*, April 14, 2015, http://blogs.cfr.org/cyber/2015/04/14/the-un-gge-on-cyber-issues-how-international-law-applies-to-cyberspace/.

[15] United Kingdom of Great Britain and Northern Ireland, *Response to General Assembly Resolution 68/243 "Developments in the Field of Information and Telecommunications in the Context of International Security"* (2014), 5, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/UK.pdf.

[16] United Nations, General Assembly, *Group of Governmental Experts*, A/68/98, 2.

of recommendations that cannot be linked with legally binding obligations such as encouraging the role of the private sector and civil society.[17]

This confusion was addressed in the 2015 iteration of the UN GGE, which brought together 20 states in order to outline additional points of agreement and to further develop the content of the 2013 report. The 2015 report[18] claims to 'significantly expand' the discussion on norms. It makes a difference between 'voluntary, non-binding' (political) norms and rights and obligations deriving from international law (legal norms). The text clarifies that the UN GGE is seeking 'voluntary, non-binding norms for responsible State behaviour' that 'can reduce risks to international peace, security and stability'. It reads as follows:

> 'Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.'[19]

As such, the report is a welcome addition to the otherwise rather ambivalent discussion on norms. And, indeed, in addition to discussing aspects of international law, the group was able to propose a comprehensive set of norms for responsible behaviour and confidence-building measures.[20] A detailed overview of these proposals and the UN GGE process is provided in chapters 6 and 7. For a useful analogue with the process of agreeing on norms for outer space, read more in chapter 8.

2.2 ITU & International Telecommunications Regulations

Although not commonly viewed as a venue for discussing norms that regulate malicious state behaviour in cyberspace, the UN's specialised agency for issues concerning ICTs – the International Telecommunication Union (ITU) – should not be disregarded. In 1988, 190 Member States of ITU were able to agree on a first set of International Telecommunications Regulations (ITRs)[21] – legal norms that then mostly addressed issues related to telephony. In 2012, the ITU convened its Member States to update the ITRs 'to establish general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the under-

[17] Ibid, 8.

[18] United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by Secretary-General*, A/70/174 (22 July 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[19] United Nations, General Assembly, *Group of Governmental Experts*, A/70/174, sec. 10.

[20] See also Henry Rõigas and Tomáš Minárik, '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law,' *Incyder News*, August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

[21] International Telecommunication Union, *Final Acts of the World Administrative Telegraph and Telephone Conference Melbourne, 1988 (WATTC-88): International Telecommunications Regulations* (Geneva: International Telecommunication Union, 1989), https://ccdcoe.org/sites/default/files/documents/ITU-881209-ITRFinalActs.pdf.

lying international telecommunication transport means used to provide such services'.[22] Global agreement was not reached as only 89 of the 144 participating Member States signed the treaty.[23] The non-signatories, mostly liberal democracies, claimed that the regulations represented a move to create a 'new layer of international Internet regulation' that would compromise the free and open Internet space.[24]

The issue of Internet governance became central, even though the ITRs under discussion appeared initially as rather neutral, technically oriented and not having a focus on norms that aim to limit state actions in cyberspace.[25] Nevertheless, the discussion was fuelled by nations which advocate for more governmental control over the current 'multi-stakeholder' Internet governance system, which they criticise as being dominated by the United States (US).[26] Among other issues of disagreement,[27] there are (contested) views suggesting that the existing governance system is facilitating malicious state activities in cyberspace,[28] hence still bringing in the arguments pertaining to the behaviour of states. The disagreement on the ITRs can thus be seen as an indication of a global political divide on issues concerning state behaviour in cyberspace. Since the controversial meeting of 2012, the role of the ITU in facilitating global agreement on cyber norms related to security and Internet governance has been rather limited.[29]

3. Prominent Multilateral Initiatives

3.1 OSCE & Confidence-Building Measures

While state-led initiatives to interpret existing or developing new legal norms have been scarce, some states have been able to agree on voluntary, politically binding confidence-building measures (CBMs) that functionally support and induce the

[22] International Telecommunication Union, *Final Acts of the World Conference on International Telecommunications (Dubai, 2012): International Telecommunication Regulations* (Dubai: International Telecommunication Union, 2012), https://ccdcoe.org/sites/default/files/documents/ITU-121412-ITRFinalActs.pdf.

[23] For the list of signatories, see: International Telecommunication Union, 'Signatories of the Final Acts: 89,' http://www.itu.int/osg/wcit-12/highlights/signatories.html.

[24] See, for example, Office of Former Chairman Genachowski, *Statement From FCC Chairman Julius Genachowski on U.S. Actions at the World Conference on International Telecommunications (WCIT)*, DA/FCC: DOC-317950 (14 December 2012), https://www.fcc.gov/document/chairman-genachowski-statement-us-actions-wcit.

[25] Nevertheless, Article 5A and 5B in the ITRs were seen as controversial by many of the non-signatories of the ITRs. Read more: 'Updating International Telecommunication Regulations at WCIT 2012: Relevant for Cyber Security?' *Incyder News*, December 19, 2012, https://ccdcoe.org/updating-international-telecommunication-regulations-wcit-2012-relevant-cyber-security.html#footnote1_c7ophq5.

[26] See, for example, Julia Pohle and Luciano Morganti, 'The Internet Corporation for Assigned Names and Numbers (ICANN): Origins, Stakes and Tensions,' *Revue française d'études américaines* 134 (2013): 29-46.

[27] See, for example, Robert Pepper and Chip Sharp, 'Summary Report of the ITU-T World Conference on International Telecommunications,' *The Internet Protocol Journal* 16 (2013), http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_16-1/161_wcit.html.

[28] Julien Nocetti, 'Contest and Conquest: Russia and Global Internet Governance,' *International Affairs* 91 (2015): 111-30.

[29] David Post, 'Stand Down! UN "Takeover of the Internet" Postponed Indefinitely,' *The Washington Post*, November 7, 2014, http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/07/stand-down-un-takeover-of-the-internet-postponed-indefinitely/; Adam Segal, 'Internet Governance after Busan,' *Council on Foreign Relations, Net Politics Blog*, November 13, 2014, http://blogs.cfr.org/cyber/2014/11/13/internet-governance-after-busan/.

establishment of norms of responsible state behaviour in cyberspace.[30] Having their roots in Cold War efforts to limit the risk of nuclear war, the general aim of CBMs as an instrument has traditionally been to prevent the outbreak of conflict by establishing practical information sharing and cooperation measures between states.[31]

Most prominently, the participating states of the Organization for Security and Co-operation in Europe (OSCE),[32] including the US and Russia, adopted a set of 11 cyber-related CBMs in December 2013.[33] The agreement includes voluntary measures facilitating cooperation by establishing communication and information sharing mechanisms: for example, the states agreed to nominate contact points to manage ICT-related incidents, to hold consultations, and to share information on their national views and policies. An Informal Working Group of representatives of participating states was assigned to oversee the implementation of the first set of CBMs and to explore the development of a second set. Against initial projections of reaching consensus in 2015, the OSCE has not yet produced a second set of CBMs as finding common ground among the 57 participating states is likely to be complicated by political tensions as well as opposing interests and ideologies. Comprehensive analysis of CBMs as an instrument for international security is provided in chapter 7.

3.2 Shanghai Cooperation Organization & 'Information Security'

If one looks at other regional actors as producers and promoters of cyber norms, the Shanghai Cooperation Organization (SCO) led by Russia and China has proven to be one of the more active. Within the organisation itself, the member states adopted the Yekaterinburg Agreement in 2009 that established the main principles and mechanisms for cooperation with regard to 'international information security'.[34] This regional agreement formed the basis for a proposal of an 'International Code of Conduct for Information Security', which was forwarded by the SCO members to the UN in 2011 and again in 2015.[35]

The Code of Conduct, which has not been put to a vote, is ultimately intended

[30] Jason Healey et al, *Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security* (Washington D.C.: Atlantic Council, 2014), www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf; République française, *Réponse de la France à la résolution 68/243 relative aux «Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale»* (2014), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/10/France.pdf.

[31] Katharina Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications* (Tallinn: NATO CCD COE Publications, 2013), https://ccdcoe.org/publications/CBMs.pdf.

[32] OSCE comprises 57 participating states including the US and Russia, see the list here: Organization for Security and Co-operation in Europe, 'Participating States,' http://www.osce.org/states.

[33] '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.

[34] Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security* (16 June 2009), https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf [Unofficial translation].

[35] 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; United Nations, General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359 (14 September 2011), https://disarmament-library.un.org/UNODA/Library.nsf/f446fe4c20839e50852578790055e729/329f71777f4b4e4e85257a7f005db45a/$FILE/A-66-359.pdf.

to apply to all UN member states, and emphasises, *inter alia*, the principle of state sovereignty with regard to its information space; it promotes a multilateral Internet management system and advocates for a stronger role for the UN in formulating international norms.[36] These notions are opposed by many Western governments, which see the code as seeking to limit the free flow of information. Furthermore, they are unwilling to implement fundamental changes to the current 'multi-stakeholder' Internet governance system,[37] and tend to focus more on existing international law and politically binding norms rather than supporting the creation of new overarching treaties. However, it should be noted that if one looks at the nature of the proposed Code of Conduct in its current form, it comprises legally non-binding norms that are of a voluntary or aspirational nature.[38]

In addition to the SCO's joint proposal to the UN, Russia has individually developed a concept for a 'Convention on International Information Security'.[39] In essence, it includes similar principles to those presented in the SCO's Code of Conduct proposed to the UN, and additionally it signals the ambition to establish a multilateral legally binding treaty regulating state activities in cyberspace. To further understand the SCO's initiatives, see chapter 9, which focuses on China's approach to cyber norms.

3.3 Other Notable International Organisations

The aforementioned forums are certainly not the only organisations where cyber norms are being developed, discussed or proposed. For instance, the Council of the European Union has emphasised the need to promote norms of responsible behaviour and confidence-building measures (i.e. politically binding norms) while strongly advocating the view that the existing international law applies to cyberspace.[40] The application of existing legal norms has also been underlined by the North Atlantic Treaty Organization.[41] Additionally, the relevance of the norms of behaviour and the applicability of international law was reiterated by the G20 in late 2015, proving once again the global acceptance of these notions.[42] The G20 Antalya Summit also showed that new politically binding norms are constantly being developed and promoted on the multilateral level, as the communiqué of the meeting included a call that states should not conduct ICT-enabled theft of intellectual property.[43]

[36] Henry Rõigas, 'An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?' Incyder News, February 10, 2015, https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html.

[37] See, for example, Pepper and Sharp, 'Summary Report of the ITU-T World Conference.'

[38] See chapter 2 by Michael N. Schmitt and Liis Vihul, 26.

[39] Ministry of Foreign Affairs of the Russian Federation, *Convention on International Information Security (Concept)* (22 September 2011), http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

[40] Council of the European Union, *Outcome of Proceedings 6122/15*: *Council Conclusions on Cyber Diplomacy*, 6122/15 (11 February 2015), http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

[41] 'Wales Summit Declaration. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales' (Declaration, North Atlantic Treaty Organization, Meeting of the North Atlantic Council, Wales, 5 September 2014), http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[42] 'G20 Leaders' Communiqué' (G20, Antalya Summit, 15-16 November, 2015), http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-_pdf/.

[43] The G20 Leaders' Communiqué of the Antalya Summit reads: ' … we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.' Ibid.

4. Bilateral Developments

In many areas, bilateral cooperation precedes multilateral agreements. Indeed, this also tends to be the case with the development of cyber norms as first progress is often made between the most advanced cyber powers. For example, the US and Russia signed an agreement on ICT-related CBMs in 2013, establishing communication lines and information exchange mechanisms with the aim to have more transparency and to avoid misperception.[44] In 2015, before the G20 Antalya meeting, the US and China were able to conclude an agreement regulating cyber activities as both governments pledged not to 'conduct or knowingly support cyber-enabled theft of intellectual property'.[45] As for other notable bilateral agreements, in the spring of 2015 Russia and China also signed a cooperation agreement on 'information security' that largely reinforces the existing agreement drawn up under the SCO.[46] In addition to agreeing on several cooperation initiatives, the Sino-Russian agreement featured an unprecedented pledge that parties will not undertake 'computer attacks' against each other.[47] These diplomatic agreements can be seen as 'expressions of goodwill' rather than firm commitments as they do not set strict legal responsibilities and therefore (so far) represent the establishment of politically binding norms.

5. Other Stakeholders: Private sector, Academia, Civil Society

Although the main focus of our book is on norms that aim to limit state activities in cyberspace, no cyber security related challenge can be solved without involving other stakeholders. One of the most prominent examples is the International Cyberspace Conference series, or the so-called 'London process', which engages governments, international organisations, businesses, civil society, and academia in discussions on key developments pertaining to the cyber domain.[48] While this

[44] The White House, Office of the Press Secretary, *FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security*, 17 June 2013, https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

[45] Ministry of Foreign Affairs of the People's Republic of China, *Full Text: Outcome list of President Xi Jinping's State Visit to the United States*, 26 September 2015, http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml.

[46] Andrew Roth, 'Russia and China Sign Cooperation Pacts,' *The New York Times*, May 8, 2015, http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0; 'The Next Level for Russia-China Cyberspace Cooperation?' *Council on Foreign Relations, Net Politics Blog*, August 20, 2015, http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/.

[47] Ibid.

[48] See description of the latest Global Conference on Cyberspace held in the Hague here: GCCS2015, 'About the Global Conference on CyberSpace 2015,' https://www.gccs2015.com/gccs/all-about-gccs2015.

and other similar conferences and workshops are certainly to be commended, their all-inclusive format is often not supportive of focused debates and delivering concrete results.[49]

Separate initiatives by stakeholder groups are noteworthy as well. Firstly, the private sector perspective is highly relevant and there are large corporations that have promoted a specific set of norms which would regulate state behaviour in cyberspace.[50] Naturally, these initiatives tend to focus on the more technical aspects of the problem and aim to limit policies that can undermine the integrity of the private sector. For industry's views on the subject, see chapters 10, 11 and Appendix 1.

Possible ideas have been also discussed within academia by scholars from disciplines ranging from computer science to political science and law. Reflecting the general international debates on the governmental level, academia presents both proposals for new norms[51] and interpretations of existing legal norms.[52] If one looks at civil society and other non-governmental organisations, international norms as such do not seem as a priority issue. However if, for example, the calls to limit ICT-enabled mass surveillance activities are regarded as promotion of a certain cyber norm, then civil society can be regarded as highly active.[53]

6. Conclusion and the Structure of the Book

This introduction – only scratching the surface of the global discussions on the topic – shows that norms play a central role in the efforts to strengthen international cyber security and stability. We see that all stakeholders agree on the baseline notions that the development of cyber technologies has created risks which should be addressed through international cooperation, and that cyber norms may be one of the most suitable vehicles for such an endeavour.

The global consensus and the acknowledgement that existing international law applies to cyberspace is certainly a necessary first step. As states have so far been less actively presenting their views on how the existing international law applies, it is especially important for academia to lead the way. Therefore, the first three articles

[49] In the (half-joking) words of the Dutch Ministry of Foreign Affairs, who closed the Hague conference, the whole event left him 'still confused, but on a higher level'. GCCS2015, *Speech Minister of Foreign Affairs Bert Koenders Closing Ceremony of the GCCS2015*, (17 April 2015), https://www.gccs2015.com/sites/default/files/documents/Closing%20speech%20Minister%20Koenders_0.pdf.

[50] See, for example, overview of Microsoft's proposals in Appendix 1. Full paper: Angela McKay, et al, Microsoft Corporation, *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* (14 December 2014), 9-11, http://www.microsoft.com/en-us/download/details.aspx?id=45031.

[51] See, for example, Duncan B. Hollis, 'An E-SOS for Cyberspace,' *Harvard International Law Journal* 52 (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1670330.

[52] Schmitt, *Tallinn Manual*.

[53] For example, for a collection of organisations focused on privacy, see Electronic Privacy Information Center, 'Online Guide to Privacy Resources,' https://epic.org/privacy/privacy_resources_faq.html.

of our book are devoted to understanding the role of legal norms. In chapter 2, Prof **Michael N. Schmitt** and **Liis Vihul** provide a comprehensive overview of the nature of the existing legal norms regulating state behaviour as they discuss treaty law, customary law, and the general principles of law in the cyber context. In chapter 3, Prof **Sean Watts** provides a more specific analysis on cyber law development by focusing on the *Law of War Manual* released by the US Department of Defense. The last article on legal norms, chapter 4, focuses on the legality of cyber espionage as Dr **Russell Buchan** presents his thought-provoking approach to the issue.

As can be seen from the on-going discussions in various bi- or multilateral settings, stakeholders tend to focus more on finding an agreement on politically binding norms. Accordingly, the second section of the book primarily takes a look at politically binding cyber norms. In chapter 5, Prof **Toni Erskine** and Dr **Madeline Carr** introduce the topic as they discuss the nature of cyber norms from the theoretical perspective of political science and international relations. Moving from theory to practice, **Marina Kaljurand** shares her thoughts on the UN GGE process by focusing on the Estonian experience and views within the Group. Chapter 7, by Dr **Patryk Pawlak**, discusses the nature of CBMs as one of the most prominent tools in contemporary cyber diplomacy, and then Prof **Paul Meyer** takes a look at the subject from a comparative perspective as he discusses the differences and similarities between the international security policy of outer space and cyberspace in chapter 8. The policy section of the book finishes with Dr **Greg Austin**'s chapter 9, where he provides a comprehensive look at the evolution of China's motivations with regard to international cyber norm development.

Although this introduction has shown that governments have a significant role in creating stability in cyberspace through agreeing on norms, the development of technologies and the corresponding ever-changing risks are still outpacing international diplomatic efforts. In order to understand the technical implications of cyber norms, the NATO CCD COE invited private sector representatives to provide their perspective on the topic. The third section of the book illustrates how the private sector views cyber norms and how their input diversifies wider international discussions. In chapter 10, Symantec's **Ilias Chantzos** with **Shireen Alam** discuss how they see cyber norms as part of a broader norm-based strategy, strongly advocating for the principle of technological integrity, and explaining the role of industry in the cyber norm creation process. Intel's Dr **Claire Vishik, Mihoko Matsubara,** and **Audrey Plonk** advocate in chapter 11 for the need for a common ontology that would support the discussions on cyber norms which are viewed only as one part of the equation. In Appendix 1 we have provided the readers with an excerpt of **Microsoft's** 2014 proposal for international cyber security norms.

Finally, we would like to express our gratitude to everyone involved in the NATO CCD COE's cyber norms project throughout the years. Foremost, we would like to thank the authors, who have shared their excellent research and ideas with the community while being extremely flexible and collaborative during the whole publication process. Our appreciation also goes to the peer-reviewers who have provided valuable feedback on the articles as well as to all the experts for participating in our workshops and helping to shape some of the ideas presented in this book. We are also grateful to our dear colleagues from the NATO CCD COE and the Estonian Ministry of Foreign Affairs who have supported the cyber norms project from the very beginning. Last but not least, we would like to thank Dr Claire Vishik who proposed the idea of publishing a book on our project during our first workshop in Stockholm in 2014.