International Cyber Norms

Legal, Policy & Industry Perspectives

Anna-Maria Osula and Henry Rõigas (Eds.)

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

This publication may be cited as:
[Article author(s)], [full article title],
International Cyber Norms: Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

NATO CCD COE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org

Print: EVG Print
Cover design & content layout: Villu Koskaru
ISBN 978-9949-9544-6-9 (print)
ISBN 978-9949-9544-7-6 (pdf)

NATO Cooperative Cyber Defence Centre of Excellence

The Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is a NATO-accredited knowledge hub, think-tank and training facility. The international military organisation focuses on interdisciplinary applied research and development, as well as consultations, trainings and exercises in the field of cyber security. The Centre's mission is to enhance capability, cooperation and information sharing between NATO, Allies and partners in cyber defence.

Membership of NATO CCD COE is open to all Allies. The Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States have signed on as sponsoring nations. Austria and Finland have joined the Centre as contributing participants. The Centre is funded and staffed by these member nations.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Foreword

All our lauded technological progress – our very civilization – is like the axe in the hand of the pathological criminal.
– Albert Einstein

Einstein's pessimistic notion is as relevant today as a century ago. The very opportunities that are created by information and communication technologies also bring vulnerabilities with them. Everything that is good and everything that is bad in human nature have their manifestations in cyberspace. The ultra-rapid advancement of technology has challenged and outpaced the development of the normative frameworks that should limit malicious activities – be it crime, hacktivism or state-sponsored activities. This book looks at these normative frameworks and focuses on the interaction between the different types of norms that regulate state behaviour in cyberspace.

International developments regarding cyber norms have been addressed by multiple international actors. NATO has taken a clear line on the issue: the Alliance expressed its position in the Wales Summit Declaration (2014), stating that existing international law applies to cyberspace. The declaration also affirmed that cyber defence is part of NATO's core task of collective defence and emphasised that a cyber attack can lead to the invocation of Article 5. Indeed, in the context of this book, Article 5 can be seen as the most relevant *norm* for the Alliance. On the global level, key players have agreed on the applicability of international law and have promoted accompanying cyber 'norms of behaviour'. First steps have been taken, but we are far from having a common understanding among states. Thus, academics and other non-state actors have *de facto* led the way on the subject of cyber norms.

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) has been addressing the subject of 'cyber norms' since its establishment in 2008. The Centre has focussed on the question of how existing international legal norms apply to cyberspace by hosting and facilitating the Tallinn Manual process. More specifically, the first *Tallinn Manual on the International Law Applicable to Cyber*

Warfare (2013) paid particular attention to cyber operations that qualify legally as 'use of force' or 'armed attack' or that take place during an armed conflict. However, since the most frequent cyber incidents do not rise to these levels, the Centre is currently finalising a follow-on project *Tallinn 2.0,* which will be published at the end of 2016.

While the Tallinn Manual process looks at the existing international law, the Centre has also taken on the task of understanding how different stakeholders conceptualise and further develop the broadly definable 'cyber norms'. This book is a result of a three-year project, during which the Centre has brought together government officials, political scientists, lawyers and industry representatives for discussions, with the aim of mapping and understanding their views on the issue. These workshops have clearly presented that different disciplines define and apply the term 'cyber norm' in various and often confusing ways. Therefore, the objective of this book is to explain, analyse and discuss these diverse approaches to cyber norms by gathering different practical and theoretical viewpoints from distinguished legal experts, political scientists, government officials and private sector representatives.

It is my hope that our work – both the Tallinn Manual process and the 'cyber norms' project – will support the efforts to agree on common norms in the cyber domain. I would like to thank the book's editors, authors, peer-reviewers and support staff for their excellent contributions to the project throughout the years.

Sven Sakkov
Director, NATO Cooperative Cyber Defence Centre of Excellence

Contents

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 publica-

tion 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.

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

CHAPTER 2

The Nature of International Law Cyber Norms[1]

Michael N. Schmitt and Liis Vihul

As with all human activity, that which takes place in cyberspace is shaped by a normative architecture consisting of related, but distinct, regimes. In the contemporary environment, policy norms loom largest, as illustrated by the issuance of national 'cyber strategies'[2] and the work of intergovernmental bodies such as the United Nations.[3] Yet, other normative regimes are also beginning to influence the development of said architecture, as demonstrated by the fervent debates in the field of ethics over the proper balance between cyber security and cyber privacy, the ever-growing body of domestic legislation to govern intrastate cyber activities, and the increasing trend in favour of setting common technical standards to foster interoperability.

This article explores the nature, formation and evolution of international legal norms pertaining to cyber activities. At present, it is fair to say that this category of norms operates in the shadow of most others, a situation often attributed to the alleged paucity of international law applicable in cyberspace. After all, very few express cyber-specific rules of international law exist. However, such assertions

1 This article was first published in the NATO CCD COE's Tallinn Papers, see Michael N. Schmitt and Liis Vihul, 'The Nature of International Law Cyber Norms,' *The Tallinn Papers* 1-9 (2014-2015).

2 See, e.g., White House, International Strategy for Cyberspace, May 11, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. For a compilation of national cyber strategies, see http://www.ccdcoe.org/strategies-policies.html.

3 See, e.g., the summary of work under the auspices of the United Nations at United Nations Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of Information Security, http://www.un.org/disarmament/topics/informationsecurity/. For a catalogue of international organisations' developments in the cyber sphere, see http://www.ccdcoe.org/incyder.html.

display a misunderstanding of the content and operation of international law that this article is, in part, designed to alleviate.

Analysis will begin by introducing and situating the different types of legal norms in the international law framework. The inquiry's foundational premise is that the rules of international law governing cyber activities are identical to those applicable to other types of conduct. Any differences in their explication and application are the product of the unique nature of cyber activities, not a variation in the legal strictures that shape their content and usage.

The article will then briefly discuss certain terminology that has befuddled discussions about international law cyber norms. This brief detour is essential because the divergent language employed by the legal and non-legal communities is a source of much confusion in discourse about the relevant norms. Such dialogue is also often obfuscated by improper reference to various norms that reside in different fields of international law that are not on point in a particular case. Experience has demonstrated that an understanding of the key legal terminology is a precondition to any meaningful interchange between the various normative communities.

With the groundwork laid for substantive analysis of international legal norms, the article turns to how they emerge, are interpreted, and develop through time. Although the analysis applies to international law generally, emphasis will be placed on two bodies of international law: that governing when states may resort to force (the *jus ad bellum*) and that applying during an armed conflict (international humanitarian law). This is because it is in these legal regimes that the law, or at least contemporary understanding of the law, applicable to cyberspace is most developed. This reality is primarily the product of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*[4] that was produced under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) between 2010 and 2013. Comprehension of how other areas of international law apply to cyber activities is far less mature, a situation being addressed by the NATO CCD COE in its ongoing 'Tallinn 2.0' project.[5]

Since legal norms reside in treaties or are found in customary international law, the examination will proceed by addressing each source of law separately, first in the abstract and then in its cyber context. Dividing the discussion of international law in this manner is useful because cyberspace poses different challenges to the formation, identification and application of each of these two sources of international law. General principles of law, which form the third source of international law, are unlikely to significantly inform the contours of international law directly applicable to cyberspace. They will therefore be addressed only briefly, before turning to the authors' final reflections on the subject.

4 *Tallinn Manual on the International Law Applicable to Cyber Warfare* [hereinafter *Tallinn Manual*], gen. ed. Michael N. Schmitt (New York: Cambridge University Press, 2013).

5 On the project, see NATO Cooperative Cyber Defence Centre of Excellence website, http://ccdcoe.org/research.html.

1. The Nature and Place of International Legal Norms

Any consideration of the international community's legal architecture, including that applicable to activities in cyberspace, necessarily begins with Article 38 of the Statute of the International Court of Justice:

> 1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
>   a. international conventions, whether general or particular, establishing rules expressly recognised by the contesting states;
>   b. international custom, as evidence of a general practice accepted as law;
>   c. the general principles of law recognized by civilised nations;
>   d. subject to the provisions of Article 59, 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.[6]

Although situated in the constitutive document of a single international tribunal, the article, which tracks the formulation found in the 1920 statute of its predecessor, the Permanent Court of International Justice,[7] is today universally accepted as accurately setting forth the three forms of international law – treaty law, customary law and general principles of law. Subparagraph (d) delineates the two secondary sources used to elucidate that law: judicial decisions and the work of distinguished scholars.[8] It must be cautioned that secondary sources are not in themselves law. In particular, and unlike the practice in many domestic jurisdictions, the decisions of tribunals are binding only on the parties before the court, a fact codified in Article 59 of the Statute. Nevertheless, such decisions and scholarly works are highly persuasive in interpreting treaty provisions and identifying customary law. Indeed, considering the lack of cyber-specific customary and treaty law, scholarly works such as the *Tallinn Manual* are proving instrumental in identifying and shaping international legal cyber norms. So too is the case law of international judicial bodies, a fact illustrated by the frequent reference herein to their pronouncements.

International legal norms differ from other inter-state norms regulating cyber behaviour in the sense that in the event of non-compliance, international legal responsibility results.[9] The essence of this responsibility lies in the obligation to stop on-going violations and to provide reparations to the injured states for the harm caused. It is therefore important to carefully distinguish legal norms from non-binding norms. For instance, a 'code of conduct', like that proposed by the

6 Statute of the International Court of Justice, art. 38, June 26, 1945, 59 Stat. 1055, 33 UNTS 993 [hereinafter ICJ Statute].
7 Statute of the Permanent Court of International Justice art. 38, Dec. 16, 1920, 6 LNTS 379.
8 See, e.g., *Oppenheim's International Law*, I, 24 (Robert Jennings and Arthur Watts eds., 9th ed. 1996).
9 Draft Articles on Responsibility of States for Internationally Wrongful Acts, art. 1, Rep. of the Int'l L. Comm'n, 53d Sess., U.N. Doc. A/56/10, GAOR 56th Sess., Supp. No. 10 (2001), reprinted in [2001] *Yearbook of the International Law Commission* 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter Articles on State Responsibility].

Shanghai Cooperation Organization,[10] seldom qualifies as international law because it is aspirational or exhortational in nature, but not compulsory. Codes of conduct or statements of best practice are not binding on states in the same manner as legal norms, and their violation does not involve the same remedies. While the sanctioning of violations of international legal norms is complicated by the general absence of a compulsory enforcement mechanism, states are nevertheless significantly more reluctant to breach legal, as opposed to other, types of norms.

Traditionally, norms of international law were viewed as binding only on states. It was left to individual states to address the conduct of individuals and organisations that fell under their personal jurisdiction when engaged in activities that were within their subject matter competency. Although international law continues to primarily govern international relations between states, in the last century it has increasingly come to address individual conduct. Classic examples include international legal norms that permit universal jurisdiction over certain acts such as war crimes. Nevertheless, to amount to international law, all such norms must be agreed to by multiple states, either through treaty or the development of customary law. In this sense, international law is at its core a body of compulsory norms involving two or more states.

As noted above, there are three forms of international law – treaty law, customary law and general principles of law. Customary law is unwritten international law that develops over time and is based on state practice. Although unwritten, it binds all states, except those that fall into a very specific and narrow category of 'persistent objector'. Treaties, by which states expressly agree to be bound in law, may be bilateral (two states) or multinational (more than two parties), and treaty law may be coterminous with customary law in the sense that a treaty's provisions simply reflect customary law, or have come to reflect customary law that has subsequently emerged. However, conceptually it is useful to think of treaty law as consisting of express agreements that either recognise customary norms or create new legal norms that render an act or failure to act unlawful for the parties to the treaty. This latter point is key since the status of the customary law governing cyber activities remains rather unsettled.

A state may even consent by treaty to certain conduct that would otherwise constitute a violation of a customary norm, unless the customary norm is of *jus cogens* character, such as the prohibition on genocide which states may never agree to violate in their relations. For instance, although certain intrusions by a state into another state's cyber infrastructure may amount to a violation of the latter's sovereignty, that state may execute a bilateral or multilateral treaty that permits other states to do so in certain circumstances, such as during joint counter-terrorism operations. Additionally, a state may acquiesce to such a violation on an *ad hoc* basis, as when it has information that its cyber infrastructure is being used for criminal purposes, but lacks the ability to address the situation itself.

10 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, Annex, UN Doc. A/66/359 (Sept. 14, 2011).

International law is typically described as prohibitory in nature: any activity that is not disallowed is generally permitted.[11] But even when law does exist, it may prove lacking when meeting unanticipated circumstances and thus is occasionally breached as part of the process of creating a new norm. Indeed, it is often said that customary law norms are 'made in the breach'. By way of illustration, it may be that pre-existing human rights law would, if logically applied in the cyber context, prohibit intrusions into certain forms of cyber communications between individuals. However, if states treat this customary norm as inconsistent with their need to ensure, for instance, the security of their cyber systems, they may begin to act contrary to the norm. Over time, their state practice, could, as will be explained, be viewed by states as legal, such that the original human rights norm will have been modified. Given the novelty of cyber activities, they are particularly vulnerable to this dynamic of customary law.

Once the international law boundaries of conduct are demarcated, domestic legal, political (policy), ethical and other norms can operate to further restrict or require particular conduct in cyberspace. For instance, while it is unclear precisely how international human rights norms in the realm of privacy restrict state monitoring of personal cyber communications, monitoring may constitute a violation of domestic constitutional law or be contrary to state policy or the ethical benchmarks that a state has adopted. Thus, international legal norms merely define the space within which states may engage in normative construction. Of course, states may act to transform these non-legal norms into those with legal authority by adopting a treaty incorporating them or engaging in state practice that crystallises over time, as described below, into customary law.

2. Terminological Precision

To avoid cross-disciplinary confusion in understanding how legal norms are created for, and applied to, cyber activities, it is first necessary to grasp the relevant legal vocabulary. Indeed, perhaps the greatest hindrance to effective conversation between cyber norm communities is terminological in nature. To cite a simple but pervasive example, non-lawyers tend to speak of 'cyber war' in a generic sense as encompassing all forms of hostile cyber activities conducted by or against states and use the term 'cyber attacks' as referring to any harmful cyber operations. However, as will be seen, these terms do not formally reside in international law. Instead, international law uses a *patois* that employs the same words – attack and war – but has a discrete normative implication.

11 *S.S. 'Lotus' (Fr. v. Turk.)*, Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 3, 18 (Sept. 7).

Of greatest significance in this regard are the legal terms of art populating the *jus ad bellum* and international humanitarian law (IHL). The *jus ad bellum* deals with the prohibition of the use of force found in Article 2(4) of the United Nations Charter and customary law, as well as the law of self-defence set forth in Article 51 and its customary law counterpart.[12] In contrast, IHL deals with how force may be employed by the parties to an armed conflict. IHL, in particular customary international law and the Geneva Conventions with their 1977 Additional Protocols,[13] contains, *inter alia,* the rules governing attacks, delineates protections to which certain persons and objects are entitled, and restricts the kinds of weapons that may be employed in order to conduct hostilities.

With respect to the *jus ad bellum*, the primary terminological obstacle deals with the use of the word 'attack'. Article 51 of the UN Charter allows states to use force in self-defence in situations amounting to an 'armed attack'. Not all hostile cyber operations directed at a state rise to this level. As a general matter (the precise threshold is by no means settled), such operations must result in the destruction of property or injury to persons before qualifying as an armed attack that opens the door to a forceful response, whether kinetic or cyber in nature.[14] Thus, for the legal community, the term 'cyber attack' in this context refers to a particularly egregious hostile cyber operation that allows for the most robust of state responses. To style operations of lesser consequences as 'attacks' often results in the various normative communities talking past each other.

In IHL, there are two consistently pernicious terminological quagmires. The first involves use of the word 'war', as in 'cyber war'. War is a historical term that no longer enjoys the normative meaning associated with it for centuries, when the fact that states were 'at war' or had engaged in an 'act of war' meant that certain bodies of law, such as the law of war and neutrality law, applied.

Since the mid-twentieth century the term has been obsolete in international law. It was intentionally discarded by the international community in lieu of 'armed conflict' in the four 1949 Geneva Conventions.[15] This was done to emphasise that international humanitarian law applies irrespective of a declaration of war or other legalistic formalities. Henceforth, the determination that states were 'at war' (involved in an armed conflict) would be factual.

It is clear that when cyber operations accompany kinetic hostilities qualifying as armed conflict (as with the conflict between Russia and Georgia in 2008 or that taking place in Syria at the time of writing), IHL applies fully to all the cyber operations

12 UN Charter, arts. 2(4) and 51.

13 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field, August 12, 1949, 75 UNTS 31; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, August 12, 1949, 75 UNTS 85; Convention (III) Relative to the Treatment of Prisoners of War, August 12, 1949, 75 UNTS 135; Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 UST 3516, 75 UNTS 287; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 UNTS 3; Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 UNTS 609.

14 *Tallinn Manual, supra* note 5, r. 13 and accompanying commentary.

15 Geneva Conventions I–IV, *supra* note 14, arts. 2 and 3.

that have a nexus to the conflict, whether they are launched by states, non-state groups or individual hackers. For instance, in the same way that IHL prohibits injurious or destructive kinetic attacks against civilians and civilian objects, it likewise prohibits cyber attacks against them having the same effects.[16]

For international lawyers the term 'cyber war' is better rendered as 'cyber armed conflict'. When non-lawyers speak of the norms applicable in cyber war, the lawyer will accordingly insist on examining the attendant circumstances, because only if they qualify as armed conflict will the specific international law norms applicable therein attach. Otherwise, the situation will be subject to those aspects of international law that apply during peacetime, such as the law of state responsibility and human rights law.

The second term that causes confusion between the normative communities is, again, 'attack'. As noted, 'armed attack' is a legal term of art in the *jus ad bellum*. Yet, 'attack' is also a legal term of art in IHL. The term does not simply refer to military operations directed by one belligerent against another during an armed conflict. Rather, it is defined in Article 49 of Additional Protocol I to the Geneva Conventions as 'acts of violence against the adversary, whether in offence or in defence'.[17] The *Tallinn Manual* accordingly defines a cyber attack as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[18]

The definition of an 'attack' lies at the core of IHL, because many of its prohibitions are framed in terms of prohibition of attacks, the paradigmatic examples being those on directing attacks against civilians and civilian objects.[19] To the extent that a cyber operation does not qualify as an attack in the IHL regime, the prohibitions are inapplicable. Consequently, when a non-lawyer uses the term 'cyber attack', clarification must be sought (in addition to the *jus ad bellum* issue outlined above) not only as to whether the operation occurred during an armed conflict such that IHL applies, but also whether the operation constitutes an attack such that IHL prohibitions and restrictions come into play.

Clearly, terminological indistinctness and imprecision have long hobbled interdisciplinary understanding between the legal and non-legal communities; they continue to do so today. A proper grasp of the international law governing cyber operations, and its likely future evolution, demands terminological fastidiousness. It is to that law that we now turn.

16 *Tallinn Manual, supra* note 5, rr. 32 and 37.
17 Additional Protocol I, *supra* note 14, art. 49(1).
18 *Tallinn Manual*, *supra* note 5, r. 30.
19 See the various prohibitions set forth in Additional Protocol I, *supra* note 14, part. IV.

3. General Rules Governing Treaty Law

As noted, international legal norms bearing on cyber activities take two forms, the most commonly recognised by the non-legal community being treaty law. A treaty is an international agreement governed by international law.[20] Such agreements adopt many titles – protocol, agreement, convention, act, etc. So long as the parties to the agreement intended to create legally binding rights and obligations for themselves, the instrument's precise appellation is of no legal significance.[21]

The law that applies to the formation, application, and interpretation of an international agreement is identical irrespective of its subject matter. The law governing treaties is in great part captured in the Vienna Convention on the Law of Treaties.[22] While some states, such as the United States (US), are not party to the Convention, most of its provisions are viewed as reflective of customary international law, a topic examined below.

Of particular note in the cyber context is the principle that treaties are governed exclusively by international law, except in cases where the agreement itself refers to domestic law. The fact that a state's domestic law or even constitutional law disallows an action required by a treaty – or demands one prohibited by a treaty – does not excuse a state's non-compliance with the terms of the treaty. Indeed, a state may refuse to enforce an international law norm in its courts on the basis of domestic legal concerns, such as constitutional law. In states such as the US that do not accept the supremacy of international over domestic law, doing so is sometimes domestically required by law. However, the violation by that state of the international legal norm remains a breach of international law attributable to the state.

Once a treaty has been successfully negotiated, states subsequently consent to be bound by it, which may occur through a number of means. Consent may be indicated through signature (but not in every case, since signature sometimes denotes only adoption), exchange of instruments, ratification, accession, or any other means that the parties agree upon.[23] State representatives sometimes sign treaties subject to ratification. In the US, for instance, treaty-making power is vested in the President, but is subject to the 'advice and consent' of the Senate.[24] In such a case, the state only becomes bound once the instrument is ratified. A state may also 'accede' to a treaty when it did not participate in the negotiations leading to its adoption. Finally, a treaty usually specifies a particular date of its entry into force or includes a provision requiring a particular number of states to ratify the treaty before it comes into effect.[25]

These procedural requirements are important with respect to the application and evolution of legal norms, because it is not unusual for a treaty to be adopted and ratified

20 Vienna Convention on the Law of Treaties art. 2(1)(a), May 23, 1969, 1155 UNTS 331.
21 *Id.*, art. 2(1)(a).
22 Vienna Convention on the Law of Treaties, *supra* note 21.
23 *Id.*, arts. 11-15.
24 US Const. art. II, sect. 2, cl. 2.
25 See, e.g., Vienna Convention on the Law of Treaties, *supra* note 21, art. 24.

by some states long before it comes into force. For instance, the Rome Statute of the International Criminal Court[26] was adopted in 1998, but only came into force when 60 states had ratified it, which did not happen until 2002. Pending a treaty coming into force, states that have signed it or otherwise expressed an intent to eventually be bound by it may not engage in activities that would defeat the treaty's object and purpose, unless they formally provide notification of their decision to not become a party thereto,[27] as was the case with the US and the International Criminal Court Statute in 2002.[28] Accordingly, the fact that a treaty has not yet come into effect does not preclude it from having some normative significance. For instance, 89 states signed the 2012 International Telecommunication Regulations Treaty[29] at the World Conference on International Telecommunications in Dubai, United Arab Emirates. From that point on they were obliged to act in accordance with the treaty's object and purpose despite the fact that it only came into effect on January 1, 2015.

States occasionally issue reservations to multilateral treaties when they consent to be bound by them.[30] Reservations act to exclude or modify treaty provisions with respect to the state concerned.[31] Some treaties prohibit reservations altogether. Even when allowed, reservations cannot be inconsistent with the object and purpose of the treaty. If a state reserves, and another state accepts the reservation, the exclusion or modification of the provision in question operates with respect to the obligations of both states. Should a party to the treaty object to the reservation, the reservation will not come into effect between the parties concerned. An objecting state may also determine that a reservation is so objectionable that the treaty is not in force at all between it and the reserving state. It should be evident that reservations to a multilateral treaty can create an extremely complex maze of legal relationships.

In addition to reservations, states may issue interpretative declarations that clarify their position with regard to a particular provision of the treaty or to how the treaty will be applied by the states concerned. Declarations have no technical legal effect on the state's rights or obligations. However, states sometimes make interpretative declarations that *de facto* amount to reservations. For example, the United Kingdom has issued a statement concerning the prohibitions on reprisals set forth in Additional Protocol I to the 1949 Geneva Conventions.[32] The statement arguably denudes certain provisions of their effect. Thus, declarations, like reservations, must always be carefully surveyed when evaluating the actual normative reach of a treaty.

Perhaps the most important aspect of treaty law deals with interpretation, as a treaty's text may be vague or ambiguous. Such ambiguity is often the only way the

26 Rome Statute of the International Criminal Court, July 17, 1998, 2187 UNTS 90.
27 Vienna Convention on the Law of Treaties, *supra* note 21, art. 18.
28 Press Statement, U.S. Department of State, Richard Boucher, Spokesman, International Criminal Court: Letter to UN Secretary General Kofi Annan, May 6, 2002, http://2001-2009.state.gov/r/pa/prs/ps/2002/9968.htm.
29 International Telecommunication Regulations, Dec. 9, 1988, S. Treaty Doc. No. 13, 102d Cong., 1st Sess. (1991).
30 Vienna Convention on the Law of Treaties, *supra* note 21, art. 19.
31 *Id*., art. 2(1)(d).
32 UK Ministry of Defence, *Manual of the Law of Armed Conflict* 422-23 (2005).

parties involved were able to achieve sufficient consensus to adopt the instrument. The Vienna Convention on the Law of Treaties provides that treaties 'shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose'.[33] The term 'context' refers to the other text of the treaty, as well as to any agreement between the parties made at the conclusion of the treaty.[34] In addition to context, interpretation of a treaty's provision should take account of any subsequent express agreement between parties as to its meaning, as well as 'subsequent practice in its application that establishes the agreement of the parties regarding its interpretation'.[35] If the meaning of a provision remains ambiguous, reference may be made to the 'preparatory work of the treaty and the circumstances of its conclusion'.[36] In other words, it is appropriate to explore what was in the mind of the parties at the time when the agreement was negotiated and adopted.

4. Treaty Law in the Cyber Context

Given that cyber activities are relatively new, very few treaties deal directly with them. Prominent contemporary examples include the Convention on Cybercrime,[37] its 2006 Additional Protocol,[38] the Shanghai Cooperation Organization's International Information Security Agreement,[39] and the ITU Constitution and Convention[40] and International Telecommunication Regulations.[41] The rules regarding treaties apply fully to each of these instruments and others that exist or are to be adopted in the future. Since it is not the purpose here to examine their substantive content, it suffices to recall that when considering the formation, interpretation and application of cyber treaty norms, the key guidance is to be found in the Vienna Convention on the Law of Treaties and in the customary law of treaties.

In light of the paucity of cyber-specific treaties, the threshold question is, of course, whether non-cyber-specific instruments even apply to cyber activities. A number of states, including Russia and China, have previously expressed some reluctance to

33 Vienna Convention on the Law of Treaties, *supra* note 21, art. 31(1).
34 *Id*., art. 31(2).
35 *Id*., art. 31(3).
36 *Id*., art. 32.
37 Convention on Cybercrime, Nov. 23, 2001, 2296 UNTS 167.
38 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Jan. 28, 2003, ETS No. 189.
39 Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security, 61st Plenary Meeting, Dec. 2, 2008.
40 Constitution and Convention of the International Telecommunication Union, Dec. 22, 1992, 1825 UNTS 330.
41 International Telecommunication Regulations, Dec. 9, 1988, deposited with the International Telecommunication Union Secretary-General. The International Telecommunication Regulations, as well as the Radio Regulations, are a legal instrument of the ITU (see Constitution of the International Telecommunication Union, art. 4(3)).

acknowledge that existing international agreements extend to cyberspace.[42] This disinclination seems to have been partially overcome in 2013 with the publication of the UN Group of Governmental Experts' (UN GGE) report, which found that '[i]nternational 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'.[43] The report also confirmed the appropriateness of the law of sovereignty and of state responsibility in the context of cyber security.[44] Both Russia and China were represented in the group. Interestingly, and unfortunately, a draft provision verbatim endorsing IHL's applicability was removed in order to secure unanimity. However, even beyond the Euro-Atlantic community, many states have publicly confirmed that IHL applies to cyber activities associated with an armed conflict.[45] There appears to be no serious opposition to the notion in academia.[46]

Considering the broad acceptance of the premise that non-cyber-specific treaty law can apply to cyberspace, an array of international agreements that govern state activities in general also constrain cyber activities. As an example, the 1982 Law of the Sea Convention delineates the type of activities that the vessels of one state may engage in while in the territorial sea of another state.[47] Although the vessels have a right of passage though the territorial sea, the passage must be 'innocent', that is, not be contrary to the interests of the coastal nation. Conducting cyber operations against the coastal state from aboard naval vessels would consequently violate the innocent passage regime for states party to the Convention, even though that treaty was adopted well before the advent of sea-based cyber operations. Similarly, the 1963 Moon Treaty provides that the Moon and other celestial bodies are to be used for 'exclusively peaceful purposes'.[48] Therefore, military cyber operations may not be launched from the moon or other celestial bodies, again despite the fact that the treaty predates the technical capability to do so. In Europe, the 1950 European Convention on Human Rights (in effect since 1953) is playing a prominent role in privacy and data protection debates involving cyber communications that its drafters could not have envisaged.[49]

42 As an example, Russia has put forward arguments that instead of regulating cyber armed conflict through IHL, it should be outlawed altogether. On this point, as well as for a comprehensive overview of Russia's views on cyber-conflict, see Keir Giles and Andrew Monaghan, *Legality in Cyberspace: An adversary view* 12 (2014), http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1193.

43 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, U.N. Doc. A/68/98, June 24, 2013, http://undocs.org/A/68/98.

44 *Id*., paras. 20-23.

45 See, e.g., Information Security Policy Council, Japan, International Strategy on Cybersecurity Cooperation 9 (Oct. 2, 2013), http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf; Australian Department of Defence, White Paper 21 (2013), http://www.defence.gov.au/whitepaper2013/docs/WP_2013_web.pdf; Republic of Korea, Report to the United Nations Secretary General 1 (2014), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/10/ROK.pdf (welcoming the report of the 3rd UN Group of Governmental Experts, 'including the agreement that existing international law is applicable in cyberspace'); Georgia, Report to the United Nations Secretary General 5 (2014), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/Georgia.pdf.

46 The International Committee of the Red Cross has endorsed the same view. ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts 37, Doc. 31IC/11/5.1.2, Oct. 31, 2011.

47 United Nations Convention on the Law of the Sea, arts. 17-19, Dec. 10, 1982, 1833 UNTS 397.

48 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, art. IV, Dec. 5, 1979, 1363 UNTS 3.

49 Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 UNTS 222.

It is, however, in the realm of treaty law dealing with the *jus ad bellum* and IHL that non-cyber-specific treaties are presently playing the most prominent role. This is because of the relative maturity of these bodies of law as compared to certain others that are implicated by cyber operations, such as the law of state responsibility. Additionally, cyber legal issues logically first attracted the attention of lawyers involved in military affairs, as it is primarily the military that plans, develops and executes cyber operations. Since these lawyers' training and experience is in conflict law, the evolutionary development of legal scholarship in conflict law before that in other fields of international law is understandable. Therefore, as of now, the normative regimes of the *jus ad bellum* and IHL offer the most fertile ground for examining how non-cyber-specific treaty law applies in the cyber context. It is certainly with respect to them that the discourse is most mature.

Central among these treaties are the UN Charter with respect to *jus ad bellum*, and the 1949 Geneva Protocols and their 1977 Additional Protocols in IHL. Given the general applicability of these instruments to cyber conflict, the key issue is how their norms are to be *interpreted* in the cyber context. This was the focus of inquiry by the International Group of Experts that prepared the *Tallinn Manual*. Although the *Tallinn Manual* embraces the premise of complete applicability of *jus ad bellum* and IHL norms,[50] it is replete with examples of circumstances in which the experts could not achieve consensus on their precise interpretation with respect to cyber operations. Accordingly, the manual often refers to majority and minority views among them. To ensure comprehensiveness, on numerous occasions the manual even acknowledges the existence of reasonable interpretations not supported by any member of the group.[51]

As became clear during the *Tallinn Manual* drafting process, the object and purpose of treaties enjoys particular significance when interpreting existing treaties in the context of new areas of activity such as cyber conflict. This is particularly so because the activities in question were in most cases beyond the contemplation of those drafting these treaties. Therefore, when applying their provisions to cyber operations, it is necessary to examine the foundational rationale underlining them, both generally and with regard to any individual provision in question.

Four prominent examples illustrate the significance of treaty interpretation, as well as its shortcomings, in the cyber context. The first deals with the meaning of the term 'use of force' in the UN Charter's Article 2(4) prohibition thereof. The object and purpose of the provision was self-evidently to limit the circumstances in which states might resort to force to resolve their differences. All of the *Tallinn Manual* experts agreed that a cyber operation by one state against another that causes injury

50 *Tallinn Manual, supra* note 5, at 3, 13. The role of human rights law is especially complicated because not all states take the same approach with respect to the extraterritoriality of treaty-based human rights norms. The US, for instance, has historically taken the position that they do not apply extraterritorially.

51 See, e.g., acknowledgement of a view by which the gap between the thresholds of a 'use of force' and an 'armed attack' is either so narrow as to be insignificant or non-existent, but which was not shared by any member of the International Group of Experts. *Id.*, para. 7 of commentary to r. 11.

or death to individuals, or damage or destruction to property, qualifies as a use of force. However, no consensus could be reached on the exact threshold at which a cyber activity crosses into the use of force. The International Group of Experts could only offer indicative factors that states are likely to consider when deciding how to legally characterise a cyber operation in this respect.[52] Delineations of factors should prove useful as states estimate how their activities will be seen by other states, as well as when they assess the actions of other states against the norm, but they are not legal criteria *per se*. The object and purpose of Article 2(4) provided a guide to interpretation in the cyber context, but not a fully comprehensive one.

Second, Article 51 of the UN Charter provides that states may use force in response to an 'armed attack'. Here, the object and purpose was to ensure that states did not remain normatively defenceless should the enforcement regime established in the Charter fail to operate as planned. But the interpretation of this article remains a source of some uncertainty and controversy because it is unclear whether the right of self-defence extends to attacks conducted by non-state actors, or whether states are limited to law enforcement measures in responding to such hostile acts. This is an issue that was brought to the forefront of international law debate in the aftermath of the 9/11 attacks against the US by al Qaeda. It is a central one with respect to cyberspace, because a non-state group's or individual's capability to launch a hostile cyber operation at a state at the armed attack level is much more likely in the cyber context than the kinetic, due to the relative ease of acquiring the expertise and equipment for a cyber armed attack compared to a kinetic one.[53]

Recently, both the US and the Netherlands have taken the position that defensive use of force in the cyber context is permissible under Article 51 even if a cyber-attack by a non-state actor cannot be attributed to another state.[54] Those states and commentators who take the more restrictive approach in applying Article 51 to terrorist strikes would likely be at least as restrictive when considering cyber operations mounted by non-state actors. This illustrates that difficulties in interpreting treaty law in the non-cyber context are highly likely to resurface in the cyber context.

It is also unclear when a cyber operation is severe enough to be regarded as an armed attack in the sense of Article 51. According to the *Tallinn Manual*, operations causing significant damage, destruction, injury or death do qualify. Inclusion of such consequences is consistent with the UN Charter's object and purpose of limiting the

52 *Id*., paras. 8-10 of commentary to r. 11.

53 The ICJ appears to have suggested that the article only applies in situations in which the activities concerned reach the level of intensity required for an armed attack and are either conducted 'by or on behalf' of a state or with a state's 'substantial involvement'. Military and Paramilitary Activities in and against Nicaragua (*Nicar. v. U.S*), 1986 I.C.J. 14, para. 195 (June 27) [hereinafter *Nicaragua*]. However, contemporary state practice, most notably that since the 9/11 terrorist attacks, appears to contradict this position. In particular, the international community unambiguously characterised the Al Qaeda attacks as triggering the United States' inherent right of self-defence. The Security Council adopted numerous resolutions recognising the applicability of the right of self-defence to attacks by non-state actors. *See, e.g*., U.N. Doc. S/RES/1368, September 12, 2001; U.N. Doc. S/RES/1373, September 28, 2001. International organisations, including NATO, and many individual states took the same approach. *See also* Tallinn Manual, *supra* note 5, at 58.

54 Secretary General, Developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/66/152, July 15, 2011, at 18; Netherlands Government Response to the AIV/CAVV Report on Cyber Warfare, http://www.aivadvies.nl/ContentSuite/template/aiv/adv/collection_single.asp?id=1942&adv_id=3016&page=regeringsreacties&language=UK.

use of force in international relations, but consensus among the International Group of Experts stopped there; the group could not agree on any 'bright line test' for determining when such harm is sufficiently 'grave' to cross the armed attack threshold.[55] Some experts took the position that the term should include operations that cause severe non-physical harm, such as cyber operations directed at crippling a state's economy.[56] Others resisted such a broad interpretation on the grounds that it ran counter to the Charter's presumption in favour of non-forceful resolution of international disputes. Again, a reliable interpretation of a treaty provision in the cyber context proved elusive because multiple reasonable interpretations were possible.

The third and fourth examples derive from IHL. The paradigmatic interpretive hurdle in IHL is that cited above, the meaning of the word 'attack', which is found in various prohibitions set forth in Additional Protocol I. For instance, pursuant to express provisions of that treaty, it is unlawful to attack civilians, civilian objects, and certain other protected persons and objects.[57] Additionally, states are required to consider expected collateral damage at the attack level when assessing the proportionality of their operations,[58] and must take precautions to minimise such damage whenever they conduct attacks.[59] Interpretation of the term 'attack' in the cyber context is essential because, to the extent to which a cyber operation fails to qualify as an attack, these and related IHL provisions do not apply.

Recall the Article 49 of Additional Protocol I definition of attack as an act of violence and the definition of cyber attack found in the *Tallinn Manual* as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'. All members of the International Group of Experts agreed that Additional Protocol I's provisions referring to attacks included such cyber operations because they were violent in the sense of Article 49. However, members of the group differed on whether, and if so how far, the notion of violence should be stretched to include operations having non-kinetic effects. Some experts were of the view that the notion is strictly limited to cyber operations that cause physical damage or injury; other operations were not violent and therefore did not qualify as attacks. But a majority of them looked to the object and purpose of the Protocol and its relevant provisions to interpret the term more liberally as applying to a situation in which the functionality of an object is affected by a cyber operation without physical damage having occurred. Illustrating the difficulties that attend the application of treaty provisions to situations that were not envisaged by the drafters, there were differences of opinion within the majority as to how 'functionality' should be interpreted.[60] As this example illustrates, layers of interpretation can exist.

55 *Tallinn Manual*, *supra* note 5, para. 6 of commentary to Rule 13, para. 8 of commentary to Rule 11.
56 *Id.*, para. 9 of commentary to Rule 13.
57 Additional Protocol I, *supra* note 14 arts. 51-56, 59.
58 *Id.*, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b).
59 Additional Protocol I, *supra* note 14, art. 57.
60 *Tallinn Manual*, *supra* note 5, paras. 4, 10-12 of commentary accompanying r. 30. On the subject, see Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack', 96 *International Review of the Red Cross* 189-206 (2014).

Finally, a similar IHL-based debate is underway as to whether the term 'civilian object' extends to data.[61] If so interpreted, a cyber operation designed to destroy civilian data would be prohibited by Article 52 of Additional Protocol I, which bans direct attacks against civilian objects. If not, civilian data is a lawful object of attack, except in those circumstances where its loss might cause physical damage to objects or injury to persons. The critical and unresolved fault line in the debate lies between interpretations that limit the term to entities that are tangible, which is arguably the plain meaning of the term 'object', and those based on the argument that in contemporary understanding the ordinary meaning of 'object' includes data.[62]

These examples illustrate that even strict application of the rules of treaty interpretation set out above fails to fully suffice in adding the requisite clarity when extant treaty provisions are applied to cyber activities. Such interpretive dilemmas are only likely to be resolved over time. Interpretive clarity will be fostered through the recurrent practice of states in application of the provisions in question, including when those states are acting in their capacity as members of international organisations like the United Nations, European Union and NATO. Also relevant will be state expressions of opinion as to proper interpretation of the terms and provisions in question. Recent examples include those proffered by former US Department of State legal adviser Harold Koh[63] and by the Dutch Government in response to the AIV report, both of which set forth state positions on the meaning of key aspects of relevant treaty law.[64] Judicial interpretation could potentially also shape the meaning of uncertain treaty norms in the cyber context, much as the judgments of the International Criminal Tribunal for the Former Yugoslavia have added significant granularity to the understanding of IHL in its non-cyber guise. Finally, the work of scholars in the field cannot be understated, in light of the stark paucity of overt state practice and interpretive pronouncements on how treaty law applies to cyber situations. This dynamic is exemplified by the exceptional influence the *Tallinn Manual* is having on the formulation of state policies with regard to the respective treaty norms that bind them.

A persistent question is whether new treaties to address cyber activities are necessary or likely to materialise. Such treaty law would undoubtedly clear much of the normative fog that presently exists, yet new treaties are fairly unlikely for the foreseeable future. Historically, treaty law tends to emerge slowly. For example, despite a millennium of sea travel and commerce, it was not until 1958 that a robust regime governing the law of the sea was codified in treaty form.[65] Similarly, although air warfare is over a century old, no treaty governing these operations exists. In both

61 Michael N. Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive Precision', 48 *Israel Law Review* 81-109 (2015).

62 *Tallinn Manual*, *supra* note 5, paras. 5 of commentary accompanying r. 38.

63 Harold H. Koh, Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland: International Law in Cyberspace (Sept. 18, 2012), 54 *Harvard International Law Journal Online* 1 (2012).

64 Dutch Government Response, *supra* note 55.

65 *See, e.g.*, Convention on the Territorial Sea and the Contiguous Zone, Apr. 29, 1958, 516 UNTS 205; Convention on the High Seas, Apr. 29, 1958, 13 UST 2312, 450 UNTS 82.

these examples, the lack of treaty law was addressed through the crystallisation of customary law norms.

In this regard, treaties governing new technologies are often crafted only after the technologies have been used for some time and have revealed lacunae or insufficiencies in the existing law. The paradigmatic examples are the conventions governing weapons such as anti-personnel landmines and cluster munitions, which were concluded decades after the first employment of the weapons and which are still the subject of much controversy.[66]

Although there are exceptions, the classic case being the adoption of space law treaties at the dawn of the space age, it must be remembered that treaties require the express consent of states. This poses numerous hurdles. First, all states are not similarly situated with respect to particular issues and, therefore, finding common ground on which states will agree to be bound can be difficult. This is certainly the case with cyber activities, in which some states are super-empowered while others are novices.

Second, in the early days of a new technology, states will be reluctant to bind themselves to particular rules until they fully understand how those rules may play out as the technology continues to develop. In particular, there is presently little support for proactively addressing cyber weaponry and cyber military operations. As with all other methods and means of warfare, states are hesitant to restrict the use of weapons that may afford them an advantage on the battlefield until they have sufficient experience to allow them to weigh the costs and benefits of prohibitions and limitations on their use.[67]

Third, to the extent that states wield cyber capabilities that are strategically or operationally useful, they have an incentive to retain the option of employing them. But those same states may be vulnerable to hostile operations by other states using similar capabilities. Therefore, it may be difficult for a state's political and legal organs to agree on how the state should characterise a particular practice, as they may view the state's national interests from different perspectives.

A fourth factor rendering cyber treaties unlikely in the near term is the difficulty of verifying compliance with their terms and effectively enforcing them. To begin with, it is sometimes difficult to even ascertain that harm is the result of a cyber operation. Not only are the technical challenges posed by attribution perplexing, but the law of attribution is complex.[68] In other words, even when the originator of a cyber operation is known, it may be unclear whether his or her actions can be deemed to be those of a state as a matter of law such that the state is in violation of a treaty obligation.

Perhaps the prospect for evolution of cyber treaty norms was best set forth by the United Kingdom in its 2013 submission to the United Nations Secretary General:

66 For instance, the US is not a party to either the Ottawa Convention on anti-personnel mines or the Dublin Treaty on cluster munitions. In both cases, it took the position that the instruments run counter to operational needs.

67 As an example, the 1923 Hague Rules of Air Warfare were never implemented in treaty form, in great part out of the uncertainty of states as to the role of air power in future conflicts.

68 On this topic, see, e.g., Michael N. Schmitt and Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution', 1:2 *Fletcher Security Review* 54 (2014).

> 'Experience in concluding these agreements on other subjects shows that they can be meaningful and effective only as the culmination of diplomatic attempts to develop shared understandings and approaches, not as their starting point. The United Kingdom believes that the efforts of the international community should be focused on developing common understandings on international law and norms rather than negotiating binding instruments that would only lead to the partial and premature imposition of an approach to a domain that is currently too immature to support it.'[69]

Even if states were to embark on multilateral diplomatic conferences with the aim of concluding cyber treaties, any resulting treaty would likely be perforated with individual reservations, thereby degrading its practical effect. While the conclusion of uniform law treaties – those requiring states to harmonise their domestic legislation by adopting the same legal norms – is usually subject to less intense negotiation than, for instance, joint security treaties that impose cyber norms directly, in the cyber context even the former have proven difficult to agree on. As an example, despite determined international promotion, the 2001 Convention on Cybercrime has been signed by only 54 states. Six of them have yet to ratify the agreement[70] and 26 reservations and 25 declarations have been attached by the states that are party to the Convention thus far. If this track record is illustrative, the prospects for crafting a meaningful legal regime specifically for cyber conflict are grim.

5. Customary International Law

The second form of international law recognised in Article 38 of the Statute of the ICJ is 'general practice accepted as law', or customary international law.[71] It is a genre of norms unique to international law in the sense that it is unwritten. In many fields, such as the law of the sea, the *jus ad bellum* and IHL, customary international law was historically predominant; only in the 20th century did treaty law on these subjects come into its own.[72]

Despite the proliferation of treaties in the last century, customary law retains its significance. In great part, this is because most treaty regimes are not universal. As an example, neither the US nor Israel are party to the 1977 Additional Protocols,

69 'Developments in the field of information and telecommunications in the context of international security,' 19, UN Doc. A/68/156, July 16, 2013, http://undocs.org/A/68/156.

70 For a list of signatories and ratifications, see *Council of Europe* website, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

71 Statute of the International Court of Justice, art. 38(1)(b), June 26, 1945, 59 Stat. 1055, 33 UNTS 993.

72 For instance, significant codification in the field occurred during the Hague Conferences of 1899 and 1907. For a list of treaties, see *International Committee of the Red Cross* website, http://www.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByDate.xsp.

although both states have been involved in numerous conflicts since their adoption. To the extent that non-party states comply with the norms expressed in a treaty, they do so only on the basis that they reflect customary international law. Also note that rules expressed in a treaty sometimes crystallise into customary law, even though they did not mirror a customary norm at the time of adoption. The classic case is that of the Regulations annexed to the 1907 Hague Convention IV.[73] When a particular point encompassed in the material scope of an agreement is not directly addressed, any existing customary law will govern the matter.[74]

Although unwritten, customary law is as binding on states as treaty law. Such law 'crystallises' upon the confluence of two factors: the objective element of state practice (*usus)*, and the subjective element of *opinio juris sive necessitatis*.[75] As noted by the ICJ in the *Asylum* case:

> 'The party which relies on custom … must prove that this custom is established in such a manner that it has become binding on the other party … that the rule invoked … is in accordance with a constant and uniform usage, practiced by the States in question, and that this usage is the expression of a right appertaining to the State … and a duty incumbent on [the other State].'[76]

Objectively, this is a high threshold. Subjectively, as this is unwritten law developed through an informal process, it is very difficult to definitively establish when crystallisation has occurred and to delineate its precise contours. For reasons that will be explained, this is particularly so with regard to nascent activities such as cyber operations.

The first prong of the test, state practice, includes both physical and verbal acts of states.[77] To qualify as state practice, the conduct in question must generally occur over an extended period of time. The classic illustration is the 1900 US Supreme Court case, *The Paquete Habana,* in which the court looked into the practice of numerous countries over a period measured in centuries to conclude that fishing vessels were exempt from capture by belligerents during an armed conflict.[78]

This temporal condition has deteriorated over time. As an example, in the *North Sea Continental Shelf* case, the ICJ, in dealing with the customary law of the sea, held that 'passage of only a short time is not necessarily a bar … [if state practice],

73 Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, October 18, 1907, 36 Stat. 2227. This was the finding of the Nuremburg Tribunal. International Military Tribunal at Nuremburg, Case of the Major War Criminals, Judgment, October 1, 1946, I Official Documents 253-54.

74 See generally Yoram Dinstein, 'The Interaction between Customary International Law and Treaties', 322 *Recueil des Cours* 383 (Martinus Nijhoff, 2007).

75 *North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.)*, 1969 ICJ. 3, paras. 71, 77 (Feb. 20); *Continental Shelf case (Libya v. Malta)*, 1985 I.C.J. 13, para. 27 (June 3); *Nicaragua*, *supra* note 54, para. 183.

76 *Asylum Case (Colom. v. Peru)*, 1950 I.C.J. 266, 276-77 (November 20).

77 *See, e.g.*, International Law Association, Final Report of the Committee on the Formation of Customary (General) International Law, Statement of Principles Applicable to the Formation of General Customary International Law, 13 ff. (2000) [hereinafter ILA Report]; I *Customary International Humanitarian Law*, xxxviii-xxxix (Jean-Marie Henckaerts and Louise Doswald-Beck, eds., 2005).

78 *The Paquete Habana*, 175 U.S. 686-700 (1900).

including that of states whose interests are specially affected [is] both extensive and virtually uniform'.[79] Perhaps the best illustration of the weakening of the requirement of long-term practice is the development of customary space law,[80] an example that suggests that the relative novelty of cyber operations does not necessarily preclude the rapid emergence of cyber-specific customary international law.

The state practice essential to establishing customary law must, even if of limited duration, be consistent. When there are significant deviations from a practice by states, which may include both engaging in an activity and refraining from one, a customary norm cannot materialise. Although minor infrequent inconsistencies do not constitute a bar to such emergence,[81] repeated inconsistencies generally have to be characterised by other states as violations of the norm in question before a customary norm can be said to exist.[82] For instance, it is clear that the prohibition on the use of force set out in Article 2(4) of the UN Charter constitutes a customary norm;[83] yet states have historically engaged in the use of force and continue to do so today. The saving factor is that when they do, their conduct is, absent the justification of self-defence, typically styled by other states as wrongful.

There is no set formula as to the number of states that must engage in a practice before a norm crystallises, although the greater the density of practice, the more convincing the argument that crystallisation has occurred.[84] Of particular importance is the diversity of the states involved on issues such as their geopolitics and legal systems,[85] and the fact that 'specially affected states' have engaged in the practice or expressed their view of such practice when engaged in by other states.[86] A specially affected state is one upon which the norm will operate with particular resonance. As an example, the International Committee of the Red Cross (ICRC) has opined that 'specially affected states' with respect to the legality of weapons include 'those identified as having been in the process of developing such weapons'.[87] In cyberspace, the US would qualify as a 'specially affected state' in light of its centrality to cyber activities and its development of military capacity in the field.

The term '*opinio juris*' refers to the requirement that a state engage in a practice, or refrain from it, out of a sense of legal obligation.[88] In other words, the state must believe that its actions are required or prohibited by international law. It is often the case that a state's behaviour is motivated by other factors, such as policy, security, operational, economic and even moral considerations. For instance,

79 *North Sea Continental Shelf*, *supra* note 76, para. 74.
80 For an early, and classic, treatment of the subject, see Myres S. McDougal, 'The Emerging Customary Law of Space', 58 *Northwestern University Law Review* 618 (1963-1964): 618-42.
81 *Fisheries Case (U.K. v. Norway)*, 1951 I.C.J. 116, 131 (December 18).
82 'In order to deduce the existence of customary rules, the Court deems it sufficient that the conduct of states should, in general, be consistent with such rules, and that instances of state conduct inconsistent with a given rule should generally have been treated as breaches of that rule, not as indications of the recognition of a new rule.' *Nicaragua*, *supra* note 54, para. 186.
83 *Id*, paras. 188-190.
84 *Customary International Humanitarian Law*, *supra* note 78, at xlii-xliv.
85 *Id*., xliv.
86 *North Sea Continental Shelf*, *supra* note 76, para. 74; ILA Report, *supra* note 78, 25-26.
87 *Customary International Humanitarian Law*, *supra* note 78, at xliv.
88 *S.S. Lotus*, *supra* note 12, at 28; *North Sea Continental Shelf*, *supra* note 76, para. 77; *Nicaragua*, *supra* note 54, para. 185 (citing).

Estonia actively seeks to maintain a clean cyber environment. It does so, not because it believes that the international legal requirement of 'due diligence' requires such measures, but rather for cyber security reasons such as to prevent the establishment and use of botets in the country. Such practices have no bearing on the creation of a customary law norm.

The fact that various norms converge to govern state conduct makes it necessary to deconstruct state practice to determine whether a state is acting out of a sense of legal obligation or is instead motivated by ethical or policy concerns. Obviously, it is often difficult to ascertain the rationale underlying a particular practice; care must be taken in drawing inferences as to *opinio juris* based solely on the existence of state practice.[89] For instance, the ICRC cited many military manuals as evidence of *opinio juris* in its 2005 Customary International Humanitarian Law study.[90] In response, the US objected that the provisions found in military manuals were often as much the product of operational and policy choice as legal obligation.[91] A similar criticism frequently attends the citation of UN General Assembly resolutions as support for the existence of a customary norm, because states can vote in favour of such legally non-binding instruments for purely political reasons. The point is that when the basis for a practice or assertion is unclear, it does not comprise the requisite *opinio juris*.

Despite this difficulty, states do engage in conduct and issue statements that clearly indicate their characterisation of certain practices as required (or not) by customary international law. As an example, although the US is a party to neither the Law of the Sea Convention nor Additional Protocol I, it often confirms that it views certain provisions of those instruments as reflective of customary international law.[92]

Once a customary norm has emerged, it is applicable to all states, including those that did not participate in the practice that led to its crystallisation. Such norms are even binding on states that are created after the customary norm has developed.[93] However, there are a number of exceptions to this general principle. In particular, a state may 'persistently object' to the norm's formation as it is emerging. If the norm nevertheless emerges, the persistent objector is arguably not bound by it.[94] In this regard, the role of 'specially affected states' is paramount.[95] It would be very unlikely

89 *North Sea Continental Shelf*, *supra* note 76, paras. 76-77.

90 *Customary International Humanitarian Law*, *supra* note 78, at xxxviii. See also *Prosecutor v. Tadić*; Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, para. 99 (Int'l Crim. Trib. for the former Yugoslavia October 2, 1995).

91 Letter to Jakob Kellinberger, ICRC, from John B. Bellinger, III and William J. Haynes II, U.S. Department of State and U.S. Department of Defense, respectively, U.S. Initial Reactions to ICRC Study on Customary International Law, November 3, 2006, http://2001-2009.state.gov/s/l/rls/82630.htm.

92 Department of the Navy and Department of Homeland Security, The Commander's Handbook on the Law of Naval Operations, paras. 1-2, NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A, 2007; The US Army Judge Advocate General's Legal Center and School, Law of Armed Conflict Documentary Supplement 232-33 (2013), http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Documentary-Supplement-2013.pdf.

93 ILA Report, *supra* note 78, at 24-25.

94 *Id.* at 27-29. The doctrine of persistent objection is not universally accepted. *Customary International Humanitarian Law*, *supra* note 78, at xlv.

95 *North Sea Continental Shelf*, *supra* note 76, para. 74.

that a customary norm could emerge over the objection of such a state. For example, given the military wherewithal of the US, and its frequent involvement in armed conflicts, it would be difficult for an IHL cyber norm to materialise in the face of a US objection thereto. Fortunately, assertions of persistent objection are infrequent; rather, disagreement regarding customary norms typically surrounds the scope of a rule, not its existence.

In certain limited circumstances, a customary norm may be regional or even local in character. To illustrate, in the *Asylum* case, the ICJ found that a regional customary norm applied in Latin America,[96] whereas in the *Rights of Passage* it determined that another existed between two states with respect to passage across India to Portuguese enclaves in that state.[97] It is foreseeable that regional norms might develop for cyber activities, particularly where states of a region are similarly situated in that regard, as in the case of Europe.

6. Customary International Law in the Cyber Context

Many obstacles lie in the path of customary norm emergence *vis-à-vis* cyberspace. The requirement of practice over time hinders this process to an extent, but is not fatal because contemporary customary international law appears to countenance relatively rapid crystallisation. A much greater impediment is the visibility of cyber activities. It is difficult to 'see' what goes on in cyberspace. Instead, the effects of cyber operations are often all that is publicly observed; in fact, sometimes even the effects are not apparent to the general public. Therefore, it can be difficult to point to a particular state's cyber practice to support an argument that a norm has emerged. States, including victim states, may be reticent in revealing their knowledge of a cyber operation, because doing so may disclose capabilities that they deem essential to their security. Undisclosed acts cannot, as a practical matter, amount to state practice contributing to the emergence of customary international law.[98]

Similarly, states will frequently hesitate to offer opinions regarding the legality of state practice in cyberspace. For instance, a state may be unwilling to definitively articulate a threshold for 'armed attack'.[99] This could be because it does not want its opponents to discern when it is likely to respond on the basis of the right of self-defence, or because it prefers not to clarify the 'use of force' threshold as doing so might limit its own options in the future. In other words, it may view strategic

96 *Asylum Case*, *supra* note 77, at 276-77.
97 *Case Concerning Right of Passage Over Indian Territory (Port. v. India)*, 1960 I.C.J. 6, p. 37 (April 12).
98 *Customary International Humanitarian Law*, *supra* note 78, at xl; ILA Report, *supra* note 78, 15.
99 As an example, at the 2014 NATO Summit in Wales, the Alliance's Heads of State and Government decided that 'A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.' – Wales Summit Declaration, Sept. 5, 2014, pt. 72, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

ambiguity as in its national interest. From an international security perspective, normative clarity is not always helpful.

Two recent examples are illustrative. The relative silence of states in reaction to the 2010 Stuxnet operation against Iranian nuclear enrichment centrifuges does not necessarily indicate that states believe that the operation was lawful (assuming for the sake of analysis that it was launched by other states, since only states can violate the prohibition on the use of force set forth in Article 2(4) of the UN Charter). On the contrary, they may have concluded that the attack violated the prohibition on the use of force because it was not in response to an Iranian armed attack pursuant to the treaty and customary law of self-defence. Yet those states may logically have decided that the operation was nevertheless a sensible means of avoiding a pre-emptive and destabilising kinetic attack against the facilities by Israel. Similarly, the 2012 Shamoon virus targeting Saudi Arabia's national oil company's computers may also have been considered a violation of the prohibition of the use of force, if it was conducted, as has been speculated, by Iran.[100] Despite this possibility, the relative downplaying by states of the legal aspects in particular, as well as the entire incident in general, may be attributable to concerns regarding the economic consequences of publicly discussing the grave consequences or the perpetrator of the operation.

It is also common for states to support or condemn a cyber activity in their international rhetoric, but not be specific as to whether the condemnation is based on customary international law or on other considerations, such as moral principles or political concerns. The PRISM surveillance programme serves as an example on point. While many states, including Germany and France, criticised the surveillance programme, with the former stating that these practices were 'completely unacceptable'[101] and the latter that they 'cannot accept this kind of behaviour from partners and allies,'[102] the comments do not necessarily confirm their position on the legality of the programme.

Other requirements that will often be difficult to meet in regard to cyber state practice are consistency and density. For instance, Brazil argued at the UN General Assembly in 2013 that the interception of communications represents 'a case of disrespect to the [country's] national sovereignty,'[103] presumably suggesting that it breaches the international law principle of sovereignty. It is unlikely that a sufficient number of other states, in particular specially affected states, will embrace the same position to the extent that the criteria of a customary norm will be satisfied.

Indeed, as noted above with regard to treaties, states may be conflicted regarding

100 Nicole Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back', *New York Times,* Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0.

101 'Merkel Calls Obama about 'US Spying on Her Phone", BBC, Oct. 23, 2013, http://www.bbc.com/news/world-us-canada-24647268.

102 'Hollande: Bugging Allegations Threaten EU-US Trade Pact', BBC, July 1, 2013, http://www.bbc.com/news/world-us-canada-23125451.

103 Statement by Brazilian President H. E. Dilma Rousseff on September 24, 2013 at the Opening of the General Debate of the 68th session of the United Nations General Assembly. Translated reprint at 2, http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

what legal position to take on cyber customary norms. As a result, they may take no position on the legality of a particular cyber practice until they fully understand the position's costs and benefits. And, of course, states will want to avoid being criticised for adopting a 'do as I say, not as I do' approach. The US, rightly or wrongly, has been the subject of such accusations with regard to its condemnation of Chinese cyber operations against US businesses.[104]

Finally, state comments regarding their own or other states' activities tend to be drafted by non-lawyers. The legal dimension of the activities is accordingly often neglected. The paradigmatic examples were the US public statements regarding possible operations against Iraq in late 2002 and early 2003, which focused on Iraq's alleged involvement in transnational terrorism and its development of weapons of mass destruction capability.[105] By the time the US finally set out its formal legal justification – a very nuanced interpretation of ceasefire law[106] – it had been rendered inaudible against the on-going geopolitical brouhaha that was underway. As this example demonstrates, international security matters generally take on policy and strategic hues, rather than legal ones. The same is proving to be true as states engage in and react to cyber activities.

Considered in concert, these factors render improbable the rapid crystallisation of new customary norms to govern cyberspace. Therefore, the normative impact of customary law on cyber conflict is most likely to take place in the guise of interpretation of existing customary norms, and if so, interpretive dilemmas similar to those affecting treaty interpretation will surface. In fact, the obstacles will be greater with respect to customary international law, because not only are the rules themselves not expressly articulated, but there are also no explicit rules regarding their interpretation such as those found in the Vienna Convention on the Law of Treaties.

7. General Principles of Law in the Cyber Context

The third formal source of international legal norms cited in Article 38 of the International Court of Justice's Statute is general principles of law. A complicating factor with respect to this source is that its nature is the subject of some controversy.[107] Generally, the term is said to refer to a number of types of legal principles that are: common across domestic legal systems, such as the use of circumstantial

104 *See, e.g.*, 'China Denounces US Cyber-theft Charges', BBC, May 20, 2014, http://www.bbc.com/news/world-us-canada-27477601.
105 Address of President George W. Bush, March 19, 2003, http://georgewbush-whitehouse.archives.gov/news/releases/2003/03/20030319-17.html.
106 Letter dated 20 March 2003 from the Permanent Representative of the US of America to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2003/351, March 21, 2003.
107 Malcolm N. Shaw, *International Law* 98 (6th ed. 2008); Oscar Schachter, *International Law in Theory and Practice* 50–55 (1991).

evidence;[108] evident from the nature of law itself, for instance *res judicata* (final judgments of a court are conclusive);[109] derive from the nature of international law, such as *pacta sunt servanda* ('agreements must be kept');[110] and based on fairness, prominent examples being equity[111] and estoppel.[112]

General principles are most likely to become relevant when disputes between states over cyber matters arise. As an example, in the celebrated *Chorzow Factory* case, the Permanent Court of International Justice held that the breach of an obligation in international law necessarily gives rise to the obligation to make reparations,[113] a principle echoed in the International Law Commission's Articles of State Responsibility.[114] Thus, if a state's cyber operations violate the sovereignty of another state and cause harm, the former will be obligated to make reparations to the latter. Similarly, courts may decide cases in part based on equitable considerations. Such a decision might be appropriate, for instance, in the case of cyber infrastructure which is shared by states.

However, at times a general principle of law may reflect a substantive obligation. The classic example is the International Court of Justice's identification of the principle that every State shoulders an 'obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[115] This pronouncement, which is now universally accepted, was the basis for *Tallinn Manual* Rule 5: 'A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States'.[116]

8. Conclusion

Legal norms are but one facet of the normative environment in which cyber operations exist. To suggest that they alone suffice would be folly. After all, there is a scarcity of cyber-specific treaty law and a near total void of cyber-specific customary law on the subject. As a result, recourse must be had to general international law and the interpretation thereof in the cyber context. Of course, any interpretive endeavour is plagued with uncertainty and ambiguity, especially when engaged in with respect to novel activities such as cyber operations. This lack of legal normative clarity invites

108 *Corfu Channel* (*U.K. v. Alb.*), 1949 ICJ. 4, at 18 (Apr. 9).
109 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. and Montenegro)*, 2007 ICJ. 43, para. 113 (Feb. 26).
110 Vienna Convention on the Law of Treaties, *supra* note 21, art. 26; AMCO v. Republic of Indonesia, 89 Int'l L. Rep. 366, 495-97 (1992).
111 *North Sea Continental Shelf*, *supra* note 76, paras. 98-99; *Barcelona Traction, Light & Power Co. Ltd. (Belg. v. Spain)*, 1970 ICJ. 3, para. 94 (Feb. 5); *Frontier Dispute (Burkino Faso v. Mali)*, 1986 ICJ 554, para. 149 (Dec. 22).
112 *Temple case*, 1962 ICJ 6, 23, 31; *Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria)*, 2002 ICJ. 275, para. 57 (Oct. 10).
113 *Chorzow Factory Case*, 1928 PCIJ., (ser. A) No. 13, at 28.
114 Articles on State Responsibility, *supra* note 10, part 2, ch. II.
115 *Corfu Channel*, *supra* note 109, at 22.
116 *Tallinn Manual, supra* note 5, r. 5.

states to take differing interpretive positions. A state's objective view of the law may drive the legal position it adopts; however, it would be naïve to deny that policy and ethical influences have an effect on such determinations.

Controversy and inexactitude will surely characterise this process, which will be neither linear nor logical. The weakening of the early Russian and Chinese objections to the application of extant international law to cyberspace is a milestone in this regard. Yet, while both states have backed away from their opening stance on the issue, it remains unclear where they stand today. Other states such as the US and the Netherlands are beginning to show a willingness to articulate their positions on how current international law applies in cyberspace. Nonetheless, the public pronouncements to date have been vague, probably intentionally so.

Despite the attention that cyber activities have drawn in the past decade, the conclusion of new treaties or the crystallisation of new customary law norms to govern them is doubtful. Opposition from western states is particularly marked to the former, at least.[117] Instead, the application and interpretative evolution of existing international law is the most likely near-term prospect. As to customary law, although it may sometimes develop rapidly, 'usually customary law is too slow a means of adapting the law to fast-changing circumstances'.[118]

Consequently, the work of scholars such as the International Group of Experts who prepared the *Tallinn Manual*, and those who are engaged in the follow-on 'Tallinn 2.0' project, is likely to prove especially influential. This dynamic is appropriate since, as noted in Article 38 of the International Court of Justice's Statute, the work of scholars is a secondary source of law that informs identification and application of primary sources. But this reality is certainly less than optimal, because states, and only states, enjoy the formal authority to make international law. Unless they wish to surrender their interpretive prerogative to academia, it is incumbent upon them to engage with cyber issues more openly and more aggressively.

In this patchwork and nebulous environment, the role of other normative regimes looms large. Only in exceptional circumstances may their dictates cross the international law border. However, where those boundaries are indistinct, common policy or ethical norms may operate to define the outer boundaries of acceptable conduct in cyberspace. Because cyber activities are a relatively new phenomenon, policy and ethical norms may serve to carve out more restrictive boundaries than international laws which are designed to constrain the other activities of states. Over time, these non-legal norms may mature through codification into treaty law or crystallise into customary law, such that they formally define the limits of cyber activities. In the meantime, cyberspace will remain an environment of fervent, and often multi-directional, normative development.

117 See, e.g., President of the US, International Strategy for Cyberspace, May 15, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 15, Doc. JOIN (2013) 1 final, February 7, 2013.

118 *Oppenheim's International Law*, *supra* note 9, at 30.

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

CHAPTER 3

Cyber Law Development and the United States Law of War Manual

Sean Watts

1. Introduction

Almost simultaneously with its emergence as a domain of military operations, cyberspace presented substantial questions concerning the application and operation of international law. A considerable body of scholarship and doctrine now exists that addresses not only the relationship between cyberspace and international law but also likely and preferable paths of cyber law development. These sources include a wide range of positions and predictions on application and development that represent the full spectrum of international law outlooks and schools of thought.

In early treatments of the subject, a viewpoint emerged that might be termed Exceptionalist. According to this view, cyberspace represented an unprecedented novelty entirely unlike other domains previously regulated by international law. Exceptionalists imagined an Internet owned and regulated by no one, over which states could not and should not exert sovereignty. Some Exceptionalist views ran so strong that they issued manifesto-like declarations of independence that defied states to intervene.[1] They advanced a view that Professor Kristen Eichensehr aptly termed 'cyber as sovereign'.[2]

1 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, (1996) accessed July 11, 2015, https://projects.eff.org/~barlow/Declaration-Final.html. *See also* David R. Johnson and David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367 (1996).

2 Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 Georgetown Law Journal 317, 326 (2015).

The Exceptionalist view rested in significant part on a conception that emphasised the virtual characteristics of cyberspace. It comprehended cyberspace as a realm entirely apart from the terrestrial and therefore territorial world governed by international law. Exceptionalists noted that cyberspace is largely ambivalent to geography and political borders. They maintained that because interactions in cyberspace are virtual, bonds of nationality and aspects of territoriality were inadequate to justify the exercise of sovereignty by states.

In response to Exceptionalists, a view developed that might be termed Sovereigntist. According to the Sovereigntist view, cyberspace, while novel with respect to the conditions that informed the creation of most existing treaties and customs, remains fully subject to international law. The Sovereigntist view continues to recognise sovereign states as both the stewards and subjects of international law in cyberspace.[3] Scholars sometimes refer in this respect to a 'cybered Westphalian age'.[4]

The Sovereigntist view rests on enduringly physical conceptions of cyberspace and an appreciation of the tangible components and groups or individuals that comprise its architecture.[5] Cyberspace, Sovereigntists emphasise, is neither virtual nor metaphysical. It is simply a collection of processors and terminals, servers and nodes, cables and transmitters – all of which are located within territorial boundaries or zones controlled by sovereign states or regulated by international legal regimes. Sovereigntists highlight that cyberspace is also designed, created, programmed and operated by people – nationals of sovereign states who are fully subject to the jurisdictional regimes of international law.

These debates concerning the role of international law in managing cyberspace spawned a cottage industry of legal commentary and scholarship seeking to influence and shape future cyber law. Overwhelmingly resolved in favour of Sovereigntists, these debates were in large part conducted by and between non-state actors such as academics, non-governmental organisations, and think tanks.[6] They produced commentary and claims that in both quantitative and qualitative terms have dwarfed the input of sovereign states.

As an example of highly influential work by non-state groups and in terms of comprehensiveness, the *Tallinn Manual on International Law Applicable to Cyber Warfare* (hereinafter *Tallinn Manual*) currently stands out from all other sources.[7]

3 *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Indiana Journal of Global Legal Studies 475 (1998) [hereinafter Goldsmith].

4 Joanna Kulesza and Roy Balleste, *Signs and Portents in Cyberspace: The Rise of* Jus Internet *as a New Order in International Law*, 23 Fordham Intellectual Property, Media and Entertainment Law Journal 1311, 1319-20; citing Chris C. Demchak and Peter Dombrowski, *Rise of a Cybered Westphalian Age*, Strategic Studies Quarterly, Spring 2011, at 32, 32. For descriptions of a similar concept see Duncan B. Hollis, *Rethinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* Jens Ohlin, Kevin Govern, and Claire Finklestein eds., 2015 Cyberwar: Law & Ethics for Virtual Conflicts 133-34.

5 *See* Jack L. Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World (2008); Goldsmith, *supra* note 121, at 476.

6 *See* Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 Texas International Law Journal 189 (2015) criticizing states' reluctance to participate in international law formation through expressions of legal opinions.

7 Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013) (hereinafter Tallinn Manual). The present author was a member of the International Group of Experts that produced the *Tallinn Manual*.

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence invited an international group of law of war experts to address the state of international law applicable to cyber warfare. In a three-year project that included unofficial consultation with select states and non-governmental organisations, the group produced the *Tallinn Manual* which identifies, in the form of rules accompanied by commentary, a broad range of cyber norms and their accompanying international legal bases. With respect to the Exceptionalist/Sovereigntist debate, the *Tallinn Manual* falls squarely in the Sovereigntist camp. Indeed, its central thesis is that cyberspace does not negate the operation of the laws of war, either *ius ad bellum* or *ius in bello*.[8]

The *Tallinn Manual* limits itself with considerable discipline to descriptive assessments of the law and assiduously avoids prescriptive arguments or advocacy. Yet its comprehensive approach and inclusive format provide fertile ground for the seeds of prescriptive claims concerning emerging law and the development of future norms. Issues on which the group could not achieve consensus are treated by commentary that records majority and minority views on a wide range of controversial subjects for which cyber norms may be emerging. Although not its purpose, the *Tallinn Manual* has inspired calls for the development of new norms, especially those identified as unsettled or ambiguous in their current state.[9]

Given their pervasiveness and in some cases persuasiveness, it is tempting to resort to the work of non-state actors, such as the *Tallinn Manual* authors, for indications of the future direction of the relationship between cyberspace and international law. Their work can easily be adopted or even mistaken as a proxy for the legal input of states. Yet the fact remains that states and states alone are responsible for and competent in the formation of international law. It will be their practices, their prerogatives, their perceptions, and, most importantly, their consent that will form future international cyber law.

In that vein, this chapter examines the recently released *United States Department of Defense (DoD) Law of War Manual*[10] (hereinafter the *Manual*) as a sample sovereign view on the current state of international norms applicable to cyberspace operations and to assess state interest in the development of new cyber-specific norms. Although its focus is on cyber operations that rise to the legal thresholds associated with or conducted in the context of armed conflict, the *Manual*'s treatment of cyber operations is a useful indication of the current state of international law development in cyberspace and offers insights into likely future developments.

Despite presenting the opportunity to do so, it will be found that the *Manual* declines to resolve considerable and relatively long-standing legal questions

8 *Id.* at 42-43, 75. In international law, the phrase *ius ad bellum* refers to the legal regime that governs states' resort to force in their international relations. *See* Marco Sassòli, Antoine Bouvier, and Anne Quintin, How Does Law Protect in War? 114-15 (3d ed., 2011). The phrase *ius in bello* describes the legal regime that regulates the conduct of hostilities during armed conflict. *Id.*

9 *See e.g.* Priyanka R. Dev, *'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 Texas International Law Journal 381, 397-400 (2015) noting legal deficiencies in cyber law as characterised by the *Tallinn Manual* and advocating refinement of legal thresholds.

10 US Department of Defense, Office of the General Counsel, Law of War Manual (2015), accessed July 27, 2015, http://www.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf (hereinafter US Law of War Manual).

concerning the operation of the law of war in cyberspace. Although they describe the US as committed to resolving unsettled and undeveloped legal issues in cyberspace,[11] the *Manual*'s authors decline to employ it as a means to stake out meaningful positions with respect to these issues or to resolve them in any significant respect. The *Manual*, with minor exceptions, is not a significant contribution to the development or refinement of cyber law. It leaves the international legal community uncertain with respect to a number of substantive legal issues in cyberspace as well as to how, if at all, the US intends to develop the law of war applicable to cyberspace.

2. The Manual and International Cyber Norm Development

The *US Law of War Manual* reflects not only the most significant expression of US views on the law of war in nearly sixty years,[12] it is also the most detailed, publicly available catalogue of US legal guidance on cyber operations since a legal assessment published by the DoD Office of General Counsel in 1999.[13] Despite frequent references to compliance with international law in a variety of policy statements and cyber strategy documents, prior to the *Manual*'s release the DoD had not issued any publicly available and generally applicable legal guidance applicable to cyber operations since the 1999 assessment.[14] And while the Legal Advisor to the US Department of State did offer highly-publicised (and closely studied) remarks on the application of international law to cyber operations at the founding of the US Cyber Command in 2012, his statements offered little in the way of specific doctrine or the operation of any particular aspect of the law of war.[15]

At its outset, the *Manual*'s chapter on cyber operations notes enduring US efforts 'to clarify how existing international law and norms … apply to cyber operations'.[16] In particular, the chapter cites US participation in a United Nations-led effort to secure state cooperation on international cyber and information security norms.[17] This UN effort, namely the periodic meetings of a Group of Governmental Experts (GGE), has touted clarifying and developing the operation of international law

11 US Law of War Manual, para. 16.1.

12 The *Manual*'s predecessor, *The Law of Land Warfare*, was published in 1956 and, with the exception of a minor 1976 addendum, served unaltered as the primary law-of-war resource of US Department of Defense lawyers until 2015. *See* US Dep't of the Army, the Law of Land Warfare, Field Manual 27–10 (July 1956).

13 US Dep't of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (November 1999), *reprinted in* 76 International Law Studies 459 (2002) (hereinafter *Legal Issues in Information Operations*).

14 *See e.g.* Office of the White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 9 (May 2011) affirming the application of international law to states' operations and activities in cyberspace.

15 US Department of State, Legal Advisor, Harold Hongju Koh, *International Law in Cyberspace*, (September 18, 2012), accessed 27 July 2015, http://www.state.gov/s/l/releases/remarks/197924.htm.

16 US Law of War Manual, *supra* note 128, para. 16.1.

17 United Nations Office for Disarmament Affairs, *Developments in the Field of Information and Telecommunications in the Context of International Security*, accessed July 27, 2015, http://www.un.org/disarmament/topics/informationsecurity.

applicable to information and communications technology as a critical component of maintaining international peace and security.[18] US participation reflects, according to the *Manual*, an important policy-based commitment to the application and relevance of international law to cyber operations.[19] As further evidence of interest in developing legal norms applicable to state behaviour in cyberspace, the *Manual* cites a Department of Defense report to the US Congress which notes that the US is 'actively engaged in the continuing development of norms'.[20] Although it is possible that the report intends to refer to other efforts or to development of political norms, it is likely that the report's reference to active engagement refers to US participation in the ongoing UN GGE process. The *Manual* does not identify any other active processes of cyber law development.

Immediately following its avowal of the US commitment to international cyber law development, however, the *Manual* includes an important qualification. Addressing the international law of war particularly, the *Manual* notes that the law is 'not well-settled, and aspects of the law in this area are likely to continue to develop'.[21] While undoubtedly accurate with respect to a number of important law of war rules, this qualification may also be an important comment on the extent to which the US considers cyber operations conclusively regulated by international law. By characterising legal issues as unsettled or undeveloped, the *Manual* may not be merely describing the state of the law as understood by DoD, it may also be signalling how the US expects to regulate cyber operations. That is, the instances the *Manual* identifies as unclear or unsettled reflect not only substantive legal evaluations, but also reflect methodological judgments about the level and nature of commitment to international law which states must demonstrate to truly commit an activity in cyberspace to international regulation. At minimum, the observation confirms the US viewpoint that a number of important regulatory ambiguities and even voids exist under the current legal framework. How and, in particular, whether to fill these gaps are crucial questions.

The *Manual*'s first substantive evaluation of how the law of war operates in cyberspace concerns a question of *ratione materiae* or what cyber situations fall within the subject matter regulated by the law of war. The *Manual* quickly dismisses the Exceptionalist view, observing that even rules developed before the advent of cyberspace are applicable to cyber operations.[22] Nothing about the structure, composition or operation of cyberspace convinces the *Manual*'s authors that cyberspace is a legal void or unregulated by existing law.

The same section on application notes 'challenging legal questions' owing to the wide range of effects, including non-kinetic effects, that cyber operations involve.

18 U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/172, (22 July 2015); G.A. Res. 69/28, para. 4, U.N. Doc. A/RES/69/28 (Dec. 11, 2014).
19 US Law of War Manual, *supra* note 10, at para. 16.1.
20 *Id*. at 994, n. 1.
21 *Id.* at para. 16.1.
22 *Id.* at para. 16.2.1.

For instance, the *Manual* notes that cyber operations which merely involve information gathering may not implicate rules applicable to attacks.[23] However the *Manual* refrains from offering any conclusive methodology, such as an effects-based approach, to resolving these questions.

In the following section, the *Manual* identifies, depending on how one tallies them, three or five principles of the *ius in bello*. The *Manual* states that '[t]hree interdependent principles – military necessity, humanity, and honor – provide the foundation for other law of war principles, such as proportionality and distinction, and most of the treaty and customary rules of the law of war'.[24] Addressing how these principles operate in cyberspace, the *Manual* notes significant ambiguity. Specifically, it indicates that cyber operations 'may not have a clear kinetic parallel in terms of their capabilities and the effects they create'.[25] Although the *Manual* does not provide an example, cyber operations that merely alter or impede the functions of a target rather than destroy it come to mind. The exact extent to which such operations implicate the *Manual*'s law of war principles is therefore unclear. The *Manual* offers no methodology or legal conclusion that would guide future analyses with respect to these questions beyond advising its audience that 'suffering, injury, or destruction unnecessary to accomplish a legitimate military purpose must be avoided'.[26] This observation suggests a role for at least one of the principles, that of military necessity, in cyber operations not clearly analogous to hostilities. But exactly which principles operate in such cases and how is left unclear.

In a departure from its nearly exclusive focus on *ius in bello* issues throughout, the *Manual* next addresses cyber operations and the *ius ad bellum*.[27] With respect to the prohibition of the use of force, the *Manual* unsurprisingly confirms that cyber operations are capable of producing effects consistent with the use of force and therefore of amounting to violations of the prohibition.[28] With respect to the 'armed attack' threshold that activates states' right to use force in self-defence, the *Manual* observes that 'any cyber operation that constitutes an illegal use of force against a state potentially gives rise to a right to take necessary and proportionate action in self-defense'.[29] Lawyers steeped in the *ius ad bellum* will recognise this very permissive characterisation of the right of self-defence as consistent with a long held US legal opinion that the 'use of force' and 'armed attack' are synonymous, an opinion that is controversial and has become increasingly isolated.[30] While a contentious legal issue, the armed attack threshold question is certainly not unique to the cyber context and therefore unlikely

23 *See e.g.* Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, arts 49-58, June 8, 1977, 1125 U.N.T.S. 3 enumerating rules and precautions that regulate 'attacks' as defined in Article 49 of the Protocol.

24 US Law of War Manual, *supra* note 10, para. 2.1.

25 *Id.* at para. 16.2.2.

26 *Id.*

27 The first chapter of the *Manual* includes an orientation to the *ius ad bellum*. *Id.* at paras. 1.11-1.11.5.6.

28 *Id.* at para. 16.3.

29 US Law of War Manual, at para.16.3.3.1

30 *See* Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. US*), 1986 I.C.J. 14, para. 191 (June 27) describing the 'use of force' and 'armed attack' as distinct legal standards with the latter reflecting more grave instances of the former.

to be resolved definitively as a purely cyber norm. Still, the *Manual*'s position equating the use of force with armed attack would seem to strengthen the need to clarify the use of force threshold with cyber examples or better yet an analytical model, an opportunity the *Manual* declines in significant part.

Importantly, the *Manual* indicates that questions concerning the legality of states' use of force by cyber means, especially in response to other actors' cyber operations, are greatly complicated by the difficulties of attribution.[31] Cyberspace offers malicious actors considerable opportunities to maintain their anonymity or to spoof the identity of other actors or states. Strong disagreement exists whether international law imposes on victim states a duty to meet a standard of proof prior to exercising self-defence. Some international lawyers argue that, prior to taking action, a responding state must achieve a requisite degree of certainty as to attribution akin to meeting an evidentiary standard in litigation as part of the law of state responsibility.[32] Others find inadequate support for the notion that states have committed anything of the sort to international law.[33] For its part, the *Manual* makes no attempt to identify, clarify, or for that matter even reject the existence of any international legal standard with respect to attribution, or to develop a cyber norm regarding this issue.

Finally, with respect to its treatment of the *ius ad bellum*, the *Manual* does not identify or discuss standards for attributing cyber operations by non-state actors to states. The significant cyber capabilities of non-state actors and the opportunity to evade attribution have induced many states to outsource their cyber operations to private groups.[34] Still, the question of non-state actor attribution is not new or even unique to cyberspace. A number of judgments by international tribunals and courts have tackled the question, producing competing standards. Specifically addressing state responsibility, the International Court of Justice (ICJ) has held that to attribute to a state the action of a non-state group that is not an organ of that state, the state in question must exercise 'effective control' over the relevant act.[35] Importantly, the effective control standard is understood to require the state to exert direct influence on

31 US Law of War Manual, *supra* note 10, at para. 16.3.3.4. *See e.g.* Choe Sang-Hun, *North Korea denies Role in Sony Pictures Hack*, New York Times, Dec. 7, 2014, http://www.nytimes.com/2014/12/08/business/north-korea-denies-hacking-sony-but-calls-attack-a-righteous-deed.html?action=click&contentCollection=Asia%20Pacific&module=RelatedCoverage&region=Marginalia&pgtype=article describing difficulty attributing 2014 hack of Sony Pictures systems.

32 *See e.g.* Mary Ellen O'Connell, *Evidence of Terror*, 7 Journal of Conflict and Security Law 22 (2002) arguing, outside the context of cyber operations, that invoking self-defence requires 'clear and convincing evidence'. *See also* Marco Roscini, Cyber Operations and the Use of Force in International Law 98-99 (2014). Roscini appears to advocate the clear and convincing evidence standard based on litigation of state responsibility claims at the International Court of Justice. *Id.* It is unclear whether Roscini regards the clear and convincing standard as applicable outside the context of ICJ litigation as a general prerequisite to lawful state exercise of self-defence. He appears to have softened his position in a recent publication; Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, 50 Texas International Law Journal 233, 250 (2015).

33 *See* Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 Villanova Law Review 569, 595 (2011) acknowledging the clear and convincing standard but resorting primarily to a general requirement of reasonableness. The *Tallinn Manual* does not include a rule identifying evidentiary standards as prerequisites to state responses.

34 *See e.g.* Michael Riley and Jordan Robertson, *Chinese State-Sponsored Hackers Suspected in Anthem Attack*, Bloomberg Business, Feb. 5, 2015, http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack describing alleged relationships between private computer hacking groups and the Chinese government.

35 Paramilitary Activities, paras. 116-17. *See also* Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz v. Serbia & Montenegro), 1996 I.C.J. 595, para. (July 11) reaffirming the Court's effective control test.

the relevant conduct of the group in question; general influence on or support for the group is not sufficient to establish attribution under the effective control standard.[36]

Since the ICJ announced its effective control standard, some have construed a less stringent standard – the 'overall control' standard used by the International Criminal Tribunal for Former Yugoslavia for purposes of applying the *ius in bello* – as a more appropriate standard for attribution, especially in cyberspace.[37] Where the effective control standard requires the state in question directly influence the specific *acts* in question, the overall control standard merely requires that the state wield general influence over the *group* or non-state actor in question. Clearly, under the overall control standard more cyber actions by more non-state actors would be attributable to more states for purposes of state responsibility or remedial action by a victim state. The *Manual*'s decision to address the *ius ad bellum* without offering guidance as to the correct legal standard for attribution is surprising and leaves the debate somewhat unresolved. As a frequent victim of malicious cyber operations by non-state actors with alleged ties to rival states, it would seem DoD would be anxious to describe or to advocate an appropriate legal standard for attribution of such acts.

In an encouraging sign of awareness, the *Manual* includes treatment of the often neglected law of neutrality. Applicable during international armed conflict, the law of neutrality outlines duties and responsibilities of both states not party to the armed conflict in question as well as belligerent states.[38] The law of neutrality has long regulated communications of belligerent parties routed through neutral territory.[39] Generally speaking, belligerent states may not erect military communications infrastructure on neutral territory.[40] However, the law of neutrality has historically permitted belligerent states to route communications through publicly available communications infrastructure located on neutral territory without imposing on neutral states any obligation to prevent such use.[41]

The *Manual* applies this relatively permissive neutrality regime in significant part to cyber operations as well. It observes, 'it would not be prohibited for a belligerent state to route information through cyber infrastructure in a neutral state that is open for the service of public messages … '. [42] With some equivocation, the *Manual* surmises that even cyber communications that carry or deliver cyber weapons or that cause destruction in a belligerent state would not be prohibited.[43] Although

36 *See* Nicholas Tsagourias, *Cyber Attacks, Self Defence and the Problem of Attribution*, 17 Journal of Conflict and Security Law 229, 238 (2012).

37 *See Prosecutor v. Tadić*, Case No. IT-94-1-A, Appeals Chamber Judgment paras. 131, 145 (Intl'l Crim. Trib. for the Former Yugoslavia July 15, 1999). *See* Scott J. Shackelford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, *in* Conference on Cyber Conflict Proceedings 2010 (Christian Czosseck and Karlis Podins eds., 2010) advocating use of the overall control standard for attribution of state responsibility in the cyber context.

38 *See generally* Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct.18, 1907, 36 Stat. 2310 (hereinafter Hague Convention V).

39 *Id.* art. 3.

40 *Id.* art. 3(a).

41 *Id.* art. 3(b).

42 US Law of War Manual, *supra* note 10, at para. 16.4.1.

43 *Id.* observing 'Thus, for example, it would not be prohibited for a belligerent state to route information through cyber infrastructure in a neutral state that is open for the service of public messages … This rule would appear to be applicable even if the information that is being routed through neutral communications infrastructure may be characterised as a cyber weapon'.

certainly a colourable interpretation of the law of neutrality, the conclusion is surprising in light of the general tenor of the law, which appears to prohibit the exercise of belligerent functions, such as attacks, through or from the territory of neutral states.[44] Whether objectively correct or not, the *Manual*'s position seems precisely the sort of stance with respect to unclear or ambiguous law needed to contribute to the development of international cyber legal norms.

Consistent with the *Manual's* general approach, the cyber operations chapter devotes the majority of its attention to the *ius in bello*. Appropriately, the first *ius in bello* issue it considers is the threshold of 'attack' in the context of cyber operations. In accordance with an apparent majority of international lawyers, the *Manual* reserves application of the *ius in bello* rules on targeting to operations that amount to an attack.[45] To illustrate, the *Manual* cites a cyber operation 'that would destroy enemy computer systems' as prohibited if directed against civilian infrastructure. The *Manual* notes that rules that apply to attacks do not apply to operations below the attack threshold and such operations may therefore be directed, consistent with the law of war, against civilians or civilian objects subject to the requirement of military necessity.[46] Examples of such operations include webpage defacement, disruption of Internet services, and dissemination of propaganda.

However, the *Manual* declines to identify comprehensive criteria or a detailed test for distinguishing cyber attacks from ordinary cyber operations. The *Manual* merely observes that cyber operations resulting only in reversible or temporary effects may not amount to an attack. A more thorough analysis or mode of scrutiny, such as that found in the *Tallinn Manual*, might have been offered (or for that matter might have been explicitly rejected) to clarify an effective international rule on the subject.[47] Worse, the *Manual* significantly confuses the issue by observing, 'A cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war'.[48] It is unclear why the described operation is not an attack if it destroys enemy property, unless perhaps the relevant destruction is incidental rather than integral to the operation or is an uncontested operation during belligerent occupation pursuant to requisition or seizure.[49]

Continuing its coverage of targeting considerations, the *Manual's* treatment of required precautions against incidental harm to civilians and civilian objects is unsurprising and consistent with longstanding US legal doctrine. However, the section includes an important observation concerning the duty to take precautions and

44 *See* Hague Convention V, *supra* note 156, arts 2-5.
45 *See e.g.* Tallinn Manual, *supra* note 125, at 106-10.
46 US Law of War Manual, *supra* note 10, at para. 16.5.2.
47 Tallinn Manual, *supra* note 125, at 106-10 addressing in commentary considerations such as effects on functionality and the nature remedial measures required to reinstate functionality as factors relevant to identifying cyber attacks.
48 US Law of War Manual, *supra* note 10, at para. 16.5.1.
49 *See* Hague Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, arts 52 and 53, October 18, 1907, 36 Stat. 2277. The law of belligerent occupation anticipates and does not prohibit requisitions and seizures of some categories of enemy property. Seizure or requisition may result in lawful destruction of some property. *Id.*

victims of cyber attacks, noting that the requirement to take feasible steps to reduce incidental civilian injury and damage is not limited to attackers.[50] The *Manual* observes that parties subject to attack must also take steps to reduce civilian harm in the event of attacks on their systems. Although the cyber operations chapter does not elaborate, a preceding chapter expands on defenders' duties in this regard.[51] The defenders' duty seems especially important and a particularly effective means of reducing civilian harm resulting from hostile cyber operations given the prevailing dual, military-civilian nature and use of the Internet and much cyber infrastructure. This section could prove exceptionally important evidence of a critical international legal norm respecting network design and use by armed forces.

Respecting the principle of proportionality,[52] and also the rule of proportionality related to precautions in attack,[53] the *Manual* offers a useful, if contestable, observation concerning assessment of incidental damage. Generally speaking proportionality prohibits attacks expected to produce 'loss of life or injury to civilians, and damage to civilian objects incidental to the attack' that would be 'excessive in relation to the concrete and direct military advantage expected to be gained'.[54] The *Manual* excludes from the notion of incidental damage, and therefore from proportionality calculations, 'mere inconveniences or temporary losses' including 'brief disruption of internet services to civilians' as well as 'economic harms in the belligerent state resulting from such disruptions'.[55] As with the preceding observations concerning defenders' duty to take precautions against harm to civilians, this observation is strong evidence of an influential state's desire to express a legal norm refined to the context of cyberspace.

A paragraph on improper use of signs offers a flurry of examples of prohibited and permissible use of disguised cyber traffic.[56] According to the *Manual*, the law of war prohibits cyber attacks 'making use of communications that initiate non-hostile relations, such as prisoner exchanges or ceasefires'.[57] In this regard the *Manual* offers helpful treatment of the question of deception that has proved critical to the success of a number of cyber operations.

The *Manual* addresses the issue of civilian participation in cyber operations as well. It notes neither a prohibition on civilian support to cyber operations of any sort, nor any prohibition on civilians' direct participation in cyber hostilities. In support of the former view, the *Manual* notes the 1949 Third Geneva Convention provision according prisoner of war (POW) status to civilians accompanying armed forces,[58] seemingly equating these civilians' POW status with an international law

50 *Id.* para. 16.5.3.
51 *Id.* at para. 5.14.
52 *See id.* at para. 2.4.
53 *See id.* para. 5.12.
54 *Id. See also* AP I, *supra* note 24, art. 51(5)(b).
55 US Law of War Manual, *supra* note 10, at para. 16.5.1.1.
56 *Id.* at para. 16.5.4.
57 *Id.*
58 Geneva Convention (III) Relative to the Treatment of Prisoners of War, art. 4A(4) August 12, 1949, 75 U.N.T.S. 135.

ratification of the legitimacy of their support to military operations.[59] With respect to the latter, the *Manual* simply notes that civilians taking direct part in cyber hostilities forfeit their protection for intentional attack by enemy forces.[60] Although an earlier section of the *Manual* includes detailed discussion of the notion of direct participation in hostilities, the chapter offers no elaboration on how the concept operates with respect to support to or conduct of cyber operations.[61]

As a final *ius in bello* matter, the cyber operations chapter considers issues associated with legal reviews of cyber weapons. The *Manual* identifies the requirement to conduct legal reviews of new weapons as a requirement of DoD policy.[62] Although an earlier chapter notes that Article 36 of Additional Protocol I to the 1949 Geneva Conventions requires state parties to conducts legal reviews of new weapons, the *Manual* declines to indicate whether the US regards the requirement as reflective of customary international law as well.[63]

The *Manual* adds a degree of clarity to the weapons review requirement by noting that '[n]ot all cyber capabilities, however, constitute a weapon or weapons system'. Yet it offers no standard by which such distinctions between cyber weapons and other code might be made. Moreover, the *Manual* declines to weigh in on whether mere alterations to existing cyber weapons are either permissible or require new legal reviews. The *Manual* appears to leave such questions to the various services of the DoD. The question is important given the mutable nature of cyber weapons and the fact that the most sophisticated cyber weapons often require frequent, even real time adjustments to ensure their effectiveness. The *Manual* might have offered significant clarification in this respect, both to its community of lawyers and to the international legal community.

3. Reflections on the Future of Cyber Norm Development

As an indication of a major power's willingness to submit to meaningful international regulation of its cyber operations, especially during armed conflict, the *Manual* offers mixed signals. On one hand, the *Manual* includes a number of statements that suggest strong US interest in refining and clarifying norms applicable to states' cyber operations. These observations and seeming commitments offer hope to those interested in resorting to international law and norms to regulate cyberspace. Moreover, the *Manual*'s cyber operations chapter is a resounding rejection of the

59 US Law of War Manual, *supra* note 10, at para. 16.5.5.
60 *Id.*
61 *Id.* at para. 5.9.
62 *Id.* at para. 16.6 citing US Dep't of Defense, Directive 5000.01, *The Defense Acquisition System*, para. E1.1.15 (May 15, 2003).
63 US Law of War Manual, *supra* note 10, at paras. 6.2.3, 16.6.

Exceptionalist view on the relationship between international law and cyberspace. The *Manual* unequivocally regards existing international law as a source of binding norms on states' conduct of cyber operations.

To a limited extent and on limited subjects, the *Manual* also follows up on US purported commitment to further cyber law development and refinement. The *Manual*'s sections on neutrality, proportionality, and precautions against civilian harm offer constructive guidance and seeming *opinio juris* on important ambiguities. Each section offers simultaneously clear expressions of applicable legal standards and useful illustrations of how those standards are understood to operate with respect to modern cyber operations.

On the other hand, the *Manual* does little of its own accord to resolve many of the unsettled and developing provisions it notes as problematic. For instance, the *Manual* resists adopting a specific analytical methodology for sorting the legal significance of cyber operations that produce effects short of destruction or violence. The *Manual* might, in relatively short order, have announced a clear position with respect to what particular cyber operations or consequences thereof relate to the *ratione materiae* of the law of war.

Similarly, the *Manual* might have staked out a clear position on the vexing issue of attribution of non-state actors' conduct to states for purposes of state responsibility, in particular for the exercise of countermeasures or self-defence. In light of the competing effective control and overall control standards, the *Manual* might have weighed in to sway, if not resolve, lingering debate on a crucial cyber norm.

The *Manual* also declines to flesh out a coherent conception of the use of force with respect to cyber operations. A quite comprehensive and systematic approach to evaluating cyber operations under the use of force standard has circulated for quite some time now and has attracted significant support.[64] That the *Manual* declines to comment in support of or against that model, is curious given the decision to address the *ius ad bellum* both generally and specifically with respect to cyber operations.

Perhaps if the *Manual* is understood to be a work primarily concerned with the *ius in bello*, the preceding decisions with respect to *ius ad bellum* and state responsibility law might be understandable. Less understandable, however, is the decision to decline to contribute normative viewpoints on a number of *ius in bello* issues relevant to cyber operations. The *Manual*'s thin treatment of the attack threshold for applying targeting rules, direct participation in cyber hostilities, and the extent and nature of the requirement to review cyber weapons reflects a clear decision not to weigh in significantly on subjects that will appear to many to be suitable for development of cyber-specific legal norms.

It is difficult to imagine the *Manual*'s authors were unaware of these unresolved issues presented by cyber operations. Its authors and reviewers, including members

64 Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Columbia Journal of Transnational Law 885 (1999) outlining a multi-criteria mode of analysis for evaluating cyber operations as use of force.

of the US DoD Law of War Working Group, are exceptionally well-informed of the current legal challenges of the cyber domain. And presented with the ambiguities identified by the *Tallinn Manual*, the *DoD Manual* faced a somewhat easier task of identifying topics the international legal community regarded as ripe for clarification. The *DoD Manual* might easily have commented favourably or otherwise on any number of the various competing majority and minority views offered by the *Tallinn* group members.

There are a number of possible explanations for the Manual's limited contributions to interpretive clarity. The first relates to methodology. In its introductory chapter, the *Manual* explains that it is not intended as a definitive work on US law of war *opinio juris*.[65] While understandable, especially considering the diffusion of responsibility within the US Government for managing its relationship to international law, the expectation that the international community will read the *Manual* as something other than an expression of *opinio juris* may be naive or even unreasonable.

A second explanation relates to timing. It is certainly possible that the *Manual*'s sparse legal refinements reflect a determination on the part of DoD that commitment to developed norms in cyberspace would simply be premature. The *Manual* incorporates by reference an observation to this effect in an early footnote, observing:

> 'The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. This is not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that precipitate legal developments, together with all their attendant policy and political considerations. … Similarly, we can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means. These are considerations that national leaders should understand in making decisions on using information operations techniques in the current formative period, but it should also be understood that the course of future events is often beyond the control of statesmen.'[66]

65 US Law of War Manual, *supra* note 10, at para. 1.1.1.
66 *Id.* at 995, n. 2.

The statement reflects an undoubtedly accurate observation of the development of international legal norms in newly emerged areas of state interaction. However, the statement was originally made with respect to cyber operations in 1999.[67] If it is true that the community of states 'does not negotiate treaties to deal with problems until their consequences have begun to be felt,' then it may be fair to question whether the problems of cyber operations remain unfelt by states fifteen years later. If uncertainties with respect to cyber operations are sufficient to prevent states from achieving legislative consensus persist and the *Manual* also evades addressing them, it seems likely that DoD regards them as still not ripe for development or resolution. That is, it may be the view of the General Counsel that activities in cyberspace should be permitted to continue to play out under these legal ambiguities before committing to clearer norms.

A third and highly pragmatic explanation relates to security classification. Although a great deal of information has been released publicly, the details of most states' cyber operations, capabilities and tactics remain highly classified. It is entirely possible that while the Manual's authors held and have perhaps even issued detailed guidance concerning the law of war and cyber operations, these views could not be published publicly without compromising highly sensitive information. Precedent for this approach can be found among US legal opinions issued with respect to detention operations early during the military campaigns that followed the attacks of September 11, 2001.[68] These highly controversial but also highly detailed and exhaustively reasoned opinions were held at extraordinarily high levels of security classification and were not released, but rather were leaked. It is not difficult to imagine that similarly detailed analyses, including clear positions on a number of legal norms, exist today in highly classified US Government legal opinions.

To be clear, none of these aspects of the *Manual* necessarily reflects shortcomings or failings. I do not wish in any respect to suggest the *Manual* or the US is under any duty or has the capacity to unilaterally clarify or perfect the international law applicable to cyber operations. There are doubtless a great number of assumptions behind the Manual's cyber chapter. Chief among them may be that the law of war applicable to cyber operations leaves many issues unresolved and therefore in some respects unregulated, and that this is often desirable. The *Manual* may simply be evidence that ambiguity from the perspective of the US is appropriate with respect to any number of legal voids.

Given the *Manual*'s enormous size, analysis and critiques have been understandably slow to emerge.[69] A fair assessment must, however, conclude that its authors

67 *Legal Issues in Information Operations*, *supra* note 131.

68 *See generally* The Torture Papers (Karen J. Greenberg and Joshua L. Dratel, eds., 2005) compiling leaked classified memos concerning detention practices of the executive branch during early stages of the Global War on Terrorism.

69 The webblog *Just Security* convened a 'mini forum' of initial reactions to the *Manual* during the summer of 2015. *See e.g.* Gary Brown, *Cyber Conflict in DOD's Law of War Manual*, Just Security (Jul. 27 2015), https://www.justsecurity.org/24950/cyber-conflict-dods-law-war-manual/; Geoffrey S. Corn, *Precautions to Minimize Civilian Harm are a Fundamental Principle of the Law of War*, Just Security (Jul. 8, 2015), https://www.justsecurity.org/24493/obligation-precautions-fundamental-principle-law-war/; Eric Jensen, *Law of War Manual: Information or Authoritative Guidance?*, Just Security (Jul. 1, 2015), https://www.justsecurity.org/24332/law-war-manual-information-authoritative-guidance.

were neither negligent nor evasive. What the *Manual* clarifies with respect to cyber operations and what it leaves unresolved should be understood simply as a snapshot of the state of international law cyber norms as well as an indication of a single state's limited interest in immediately cultivating more developed and meaningful international norms in that area. More than simply confirmation of persistent ambiguities in the operation of the law of war in cyberspace, the ambiguities the *Manual* leaves unresolved are strong evidence of the US' comfort with these uncertainties and legal voids. Alongside the halting and fitful UN GGE process for development of international cyber norms, the *Manual* indicates significant state reticence toward and even a present inclination against definitive clarity and precision in this challenging domain of state competition.

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

CHAPTER 4

The International Legal Regulation of State-Sponsored Cyber Espionage

Russell Buchan

1. Introduction

States are highly competitive actors and the competitiveness that exists between them has become increasingly intensified as the world order has become ever more globalised. In order to be successful and prosperous in this competitive environment states require access to reliable intelligence that reveals the strengths and weaknesses of their competitors.[1] Knowledge is power, after all.

A significant amount of intelligence collected by states is from sources which are publically available. Espionage is a prevalent method of gathering intelligence and describes 'the consciously deceitful collection of information, ordered by a government or organisation hostile to or suspicious of those the information concerns, accomplished by humans unauthorised by the target to do the colleting'.[2] Espionage, then, is the unauthorised collection of non-publically available information. The act of espionage can be committed through various methods. In its traditional conception, espionage describes the practice whereby a state dispatches an agent into the physical territory of another state in order to access and obtain confidential

1 'Responsible leaders in every nation seek knowledge – and, ideally foreknowledge – of the world around them. For with a better understanding of global affairs, they are apt to protect and advance more effectively the vital interests of their citizens'; Loch K. Johnson, *Secret Agencies: US Intelligence in a Hostile World* (Yale University Press, 1998), 1.

2 Geoffrey B. Demarest, 'Espionage in International Law,' *Denver Journal of International Law and Policy* 24 (1996): 326.

information.[3] States have, however, exploited technological developments in order to devise more effective methods through which to conduct espionage. Since the emergence of vessels, aeroplanes and celestial bodies, the sea, the skies and outer space have all been used as platforms to engage in (often electronic) surveillance of adversaries; that is, to commit espionage from afar.[4] It therefore comes as no surprise that since its creation cyberspace has also been harnessed as a medium through which to commit espionage.[5] Indeed, the exploitation of cyberspace for the purpose of espionage has emerged as a particularly attractive method to acquire confidential information because of the large amount of information that is now stored in cyberspace and because cyberspace affords a considerable degree of anonymity to perpetrators of espionage and is thus a relatively risk free enterprise.

Unsurprisingly, espionage has 'metastasised'[6] since the emergence of cyberspace and reports suggest that 'cyber espionage projects [are] now prevalent'.[7] As an illustration, in February 2013 the Mandiant Report identified China as a persistent perpetrator of cyber espionage.[8] In fact, the report claims that a cyber espionage entity known as Unit 61398 has been specifically created by the Chinese government and is formally incorporated into the Chinese People's Liberation Army. The Report suggests that Unit 61398 is responsible for organising and instigating a massive cyber espionage campaign against other states and non-state actors, seeking to exploit vulnerable computer systems in order to access sensitive and confidential information with the aim of bolstering China's position in the international political and economic order.

Only 4 months later in June 2013 cyber espionage was again thrust firmly into the international spotlight when Edward Snowden, a former contractor for the US National Security Agency (NSA), disclosed through WikiLeaks thousands of classified documents to several media entities including *The Guardian* and *The New York Times*. The documents were alleged to reveal that the NSA had been engaged in a global surveillance programme at the heart of which was the collection of confidential information that was being stored in or transmitted through cyberspace. In particular, the allegations were that the NSA had been engaged in a sustained and widespread campaign of intercepting and monitoring private email and telephone communications. This cyber espionage allegedly targeted numerous state and non-state actors, including officials of international organisations such as the EU, state organs (including heads of state such as

3 The use of individuals to obtain information is referred to as human intelligence (HUMINT).

4 Obtaining information by communications intercepts or other electronic surveillance is referred to as signals intelligence (SIGINT).

5 Cyber espionage is defined as '[o]perations and related programs or activities conducted … in or through cyberspace, for the primary purpose of collecting intelligence … from, computers, information or communication systems, or networks with the intent to remain undetected'; Presidential Policy Directive/PPD-20, *U.S. Cyber Operations Policy* (October 2012), http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.

6 David Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Technologies,' *AJIL Insights*, March 20, 2013, http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving.

7 Pete Warren, 'State-Sponsored Cyber Espionage Projects Now Prevalent,' *The Guardian*, 30 August, 2012, http://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent.

8 Mandiant Intelligence Center Report, *APT1: Exposing One of China's Cyber Espionage Units*, 19 February, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

German Chancellor Angela Merkel and Israeli Prime Minister Ehud Olmut), religious leaders (the Pope), companies (such as the Brazilian oil company Petrobas), non-governmental organisations (including UNICEF and Médecins du Monde) and individuals suspected of being involveed in international terrorism.[9]

In light of the scale and intensity of cyber espionage in contemporary international relations commentators have claimed that 'cyber espionage is more dangerous than you think'.[10] Important questions are now rightly being raised as to whether cyber espionage is a permissible cat-and-mouse exercise that is part of the ebb and flow of a competitive international environment, or whether it is a pernicious practice that undermines international cooperation and is prohibited by international law. This article assesses the international legality of transboundary state-sponsored cyber espionage and therefore further contributes to the ongoing discussion of which and to what extent international legal rules regulate malicious transboundary cyber operations.[11]

This article is structured as follows. Section 2 identifies the international law implicated by cyber espionage. In section 3, I argue that when cyber espionage intrudes upon cyber infrastructure physically located within the territory of another state, such conduct constitutes a violation of the principle of territorial sovereignty. In section 4, I contend that where a state stores information outside of its sovereign cyber infrastructure or transmits its information through the cyber architecture of another state, the appropriation of that information can, in sufficiently serious circumstances, amount to a violation of the non-intervention principle. Section 5 assesses whether the seemingly widespread state practice of espionage has given rise to a permissive rule of customary international law in favour of espionage generally and cyber espionage in particular. Section 6 offers some conclusions.

2. Cyber Espionage and International Law

The general starting point for determining the international legality of state conduct is the well-known *Lotus* principle.[12] Stated succinctly, this principle provides that international law leaves to states 'a wide measure of discretion which is limited only in certain cases by prohibitive rules' and that in the absence of such rules

9 For an overview of the Snowden revelations see, Ed Pilkington, 'The Snowden Files – Inside the Surveillance State,' *The Guardian*, 2 December, 2013, http://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden.

10 David Fidler, 'Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous than You Think,' *International Journal of Critical Infrastructure* 5 (2012): 29.

11 The focus of this chapter is upon the international legality of state-sponsored cyber espionage. Non-state actors such as companies are also frequent perpetrators of cyber espionage. Time and space limitations mean however that my analysis is restricted to acts of cyber espionage that are legally attributable to states under the rules on state responsibility.

12 The Case of S.S. 'Lotus' (France v. Turkey), ser. A. - No. 10 Publications of the PCIJ (Permanent Court of International Justice 1927). Interestingly, in the Kosovo Advisory Opinion, Judge Simma referred to the Lotus principle as an 'old, tired view of international law'; Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion (Declaration of Judge Simma), ICJ Reports 2010, p. 403, para. 2.

'every State remains free to adopt the principles which it regards best and most suitable'.[13]

There is no specific international treaty that regulates cyber espionage. There is also no specific international treaty that regulates espionage and which could be adapted to regulate cyber espionage.[14] However, in an international legal order premised upon the sovereign equality of states,[15] it is inherent in the nature of an intrusive transboundary activity such as cyber espionage that this type of conduct can run into conflict with general principles of international law. In this sense, whilst cyber espionage is not specifically regulated by international law it may be nevertheless unlawful when appraised against general principles of international law.

The principle of state sovereignty is often regarded as a constitutional norm of international law and is the basis 'upon which the whole of international law rests'.[16] However, '[s]overeignty has different aspects'[17] and in order to protect the different features of state sovereignty the international community has developed various principles of international law. These include the principle of territorial sovereignty, which protects the territory of a state from external intrusion;[18] the principle of non-intervention, which protects the political integrity of a state from coercion;[19] the prohibition against the use of force,[20] which protects states against the use of violence, and where the use of violence is of sufficient scale and effects international law casts such conduct as an armed attack entitling the victim state to use force in self-defence.[21] Given that cyber espionage does not involve the use of violence, this chapter will not consider whether cyber espionage can amount to a use of force or an armed attack. Instead, my focus will be upon whether cyber espionage violates the principles of territorial sovereignty and non-intervention.[22]

13 The Case of S.S. 'Lotus', paras. 18-19.

14 At least during times of peace. Espionage, and by extension cyber espionage, committed during times of armed conflict is subject to Article 46 of Additional Protocol 1 (1977) to the Geneva Conventions (1949). See *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (8 June 1977), Article 46, https://www.icrc.org/ihl/INTRO/470. This chapter, however, concerns the international legality of cyber espionage committed outside of armed conflict.

15 United Nations, *Charter of the United Nations* and *Statute of the International Court of Justice* (24 October 1945), 1 UNTS XVI, Article 2(1).

16 Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 14 Reports of Judgments, para. 263 (International Court of Justice 1986).

17 Robert Jennings and Adam Watts, eds., *Oppenheim's International Law*, 9th edn (London: Longman, 1996), 382.

18 The Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania), 1, 35 Reports of Judgments (International Court of Justice 1949).

19 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 202.

20 United Nations, *Charter of the United Nations*, Article 2(4).

21 Ibid, Article 51.

22 Whether cyber espionage contravenes international human rights law is outside of the scope of this chapter. On cyber espionage and international human rights law see David Fidler, 'Cyberspace and Human Rights,' in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2015).

3. The Principle of Territorial Sovereignty

Sovereignty denotes *summa potestas* – the capacity to exercise full and exclusive authority. In international law the emergence of the concept of sovereignty 'coincided with the emergence of the State as a political unit following the apportionment of territories and the political and legal recognition of such territorial compartmentalisation by the Treaty of Westphalia'.[23] As a result, sovereignty is typically understood as the right of states to exercise exclusive authority over their territory. As Arbitrator Max Huber explained in the *Island of Palmas* Arbitration Award, '[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right therein, to the exclusivity of any other States, the functions of a State'.[24] In the words of the International Court of Justice (ICJ) in the *Corfu Channel* case, '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations'.[25] There is thus little doubt that the principle of territorial sovereignty is firmly entrenched in international law.

In order to constitute a violation of the principle of territorial sovereignty is the mere intrusion into a state's territory unlawful or, in addition, must the intrusion produce physical damage?[26] This is an important question in the context of cyber espionage because this is a practice that describes the accessing and copying of confidential information and is committed regardless of whether information is lost or damaged (in the sense that it is modified or deleted); in short, cyber espionage cannot be said to produce physical damage.

Wright argues for a broad definition of the principle of territorial sovereignty which does not require the infliction of physical damage. Writing in the context of traditional espionage, Wright explains that:

> '[i]n times of peace … espionage and, in fact, any penetration of the territory of a state by agents of another state in violation of the local law is also a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states.'[27]

23 Nicholas Tsagourias, 'The Legal Status of Cyberspace,' in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2015), 17.

24 Island of Palmas Case (Netherlands v. USA), 2 RIAA 829, 838 (Perm. Ct. Arb. 1928).

25 The Corfu Channel Case, 35.

26 The Commentary to the *Tallinn Manual* explains that the International Group of Experts agreed that an intrusion into the territory of another state which causes physical damage results in a violation of territorial sovereignty but notes that there was 'no consensus' between the experts as to whether intrusion into territory that does not produce physical damage also represents a violation; Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 16.

27 Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs,' in *Essays on Espionage and International Law*, ed. Richard Falk (Ohio State University Press, 1962), 12. '[The principle of territorial integrity] negates the general permissibility of strategic observation in foreign territory'; John Kish and David Turns, *International Law and Espionage* (Boston: Martinus Nijhoff, 1995), 83.

It is on the same basis that the use of reconnaissance aeroplanes in the territorial airspace of another state is generally accepted as an unlawful infraction of the territorial sovereignty of that state.[28]

Importantly, there is support for this broad interpretation of the principle of territorial sovereignty within international jurisprudence. In the *Lotus* case the Permanent Court of International Justice explained that the 'first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State'.[29] In the *Corfu Channel* case the ICJ determined that the UK's decision to send warships into Albania's territorial waters to collect evidence of illegal mining represented an unauthorised incursion into Albania's territory and thus 'constituted a violation of Albanian sovereignty'.[30] Although physical evidence was collected from Albanian territory, a careful reading of the ICJ's judgment reveals that the Court determined that the UK's conduct was unlawful solely on the basis of its unauthorised intrusion into Albania's territorial sea.

The weight of evidence, then, suggests that a violation of territorial sovereignty occurs where a state makes an unauthorised intrusion into the territory of another state, regardless of whether physical damage is caused.[31]

Turning now to the international legality of transboundary cyber conduct, the initial question is whether states possess territorial sovereignty in cyberspace. At its creation commentators asserted that cyberspace was an a-territorial environment and, because of the interdependent relationship between territory and sovereignty (territory contains sovereign power within strictly defined physical parameters), international legal concepts such as territorial sovereignty were not applicable to cyberspace.[32]

In light of state practice, however, '[t]he argument that cyberspace constitutes a law-free zone is no longer taken seriously'.[33] In particular, state practice clearly reveals that states regard themselves as exercising sovereignty in cyberspace.[34]

---

28 'The principle of the respect for territorial sovereignty is also directly infringed by the unauthorized overflight of a State's territory by aircraft belonging to or under the control of the government of another State'; Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 251.

29 The Case of S.S. 'Lotus', paras. 19-20.

30 The Corfu Channel Case, 35.

31 '[D]amage is irrelevant and the mere fact that a State has intruded into the cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty'; Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' *International Law Studies* 89 (2013): 129. For the opposing view that physical damage is required see Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law,' in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,* ed. Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2013), 458.

32 David Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace,' *Stanford Law Review* 48 (1996): 1367.

33 For a discussion of this state practice see Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' *Baltic Yearbook of International Law* 14 (2014): 142.

34 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 the Secretary-General*, A/68/98 (24 June 2013), paras. 19-20, https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf; 'Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyberspace': The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), 9, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; see also Schmitt, *Tallinn Manual*, Rule 1.

Moreover, states assert that they exercise *territorial* sovereignty in cyberspace.[35] Although on the face of it cyberspace would appear immune from territorial sovereignty because it is a virtual, borderless domain, it must nevertheless be appreciated that cyberspace is a man-made environment that 'requires physical architecture to exist',[36] including fibre-optic cables, copper wires, microwave relay towers, satellite transponders, Internet routers etc. As a result, where computer networks are interfered with, or where information is interfered with that is located on those networks, and those networks are supported by cyber infrastructure physically located in a state's territory, that state's territory can be regarded as transgressed and thus a violation of the principle of territorial sovereignty occurs.[37] Note that the key issue is not to whom the cyber infrastructure belongs but whether it is located on the territory of the state: 'it is irrelevant whether the cyber infrastructure protected by the principle of territorial sovereignty belongs to or is operated by government institutions, private entities or private individuals'.[38]

In relation to cyber espionage specifically, as I noted in the introduction to this article there has been a dramatic increase in this practice in recent years. State practice in this area is instructive and indicates that where computer systems are accessed and information is obtained that is resident on or transmitting through those computer networks, states consider their territorial sovereignty violated where those networks are supported by cyber infrastructure located within their territory. To put the same matter differently, there is state practice to suggest that where a state considers itself to have been the victim of cyber espionage it regards such behaviour as falling foul of the principle of territorial sovereignty.

For example, when it was revealed that the US had routinely committed cyber espionage against Brazil, Brazilian President Dilma Rousseff cancelled a scheduled visit to Washington DC to meet representatives of the Obama administration to discuss important issues of international concern. Instead, she proceeded to New York to formally denounce the NSA's activities before the UN General Assembly. Indeed, in doing so she explained that cyber espionage violates state sovereignty:

> 'intrusion [and] [m]eddling in such a manner in the life and affairs of other countries is a breach of international law [and] as such an affront to the principles that must guide the relations among them, especially among friendly nations. A country's sovereignty can never affirm itself to the detriment of another country's sovereignty.'[39]

35 For a discussion of this state practice see von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' 126 ('State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty'). For further discussion see Sean Kanuck, 'Sovereign Discourse on Cyber Conflict under International Law,' *Texas Law Review* 88 (2010): 1571.

36 Patrick W. Franzese, 'Sovereignty in Cyberspace: Can it Exist?' *Air Force Law Review* 64 (2009): 33.

37 Rule 1 of the Tallinn Manual explains that '[a] State may exercise control over cyber infrastructure and activities within its sovereign territory': Schmitt, *Tallinn Manual*.

38 Von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' 129. For a similar view see Schmitt, *Tallinn Manual*, 16.

39 Quoted in Julian Borger, 'Brazilian President: US Surveillance a 'Breach of International Law,' *The Guardian* September 24, 2013, http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

The President further noted that Brazil's objections to such 'illegal actions' had been communicated to the US by 'demanding explanations, apologies and guarantees that such acts or procedures will never be repeated again'.[40] Germany also stated that the conduct was 'completely unacceptable',[41] with France claiming that it 'cannot accept this kind of behaviour from partners and allies'.[42] China adopted a similar position, determining that the NSA had 'flagrantly breached international laws, seriously infringed upon the [sic] human rights and put global cyber security under threat'.[43] China further declared that the NSA's conduct 'deserve[d] to be rejected and condemned by the whole world'.[44]

The Snowden revelations have provoked a considerable international backlash from the international community and much of this criticism has been from a political, moral and even economic perspective. Schmitt and Vihul therefore correctly suggest that we approach state reactions to the Snowden revelations with caution because their 'comments do not necessarily confirm their position on the legality of the [surveillance] programme'.[45] International relations are of course complex and operate on various different levels and it is therefore necessary to approach state responses to international events cautiously and we need to be careful not to overstate the international legal significance of their claims. For example, France's claim that it 'cannot accept this kind of behaviour from partners and allies' can perhaps be interpreted in a variety of ways and such a statement does not unambiguously indicate that France considered the NSA's conduct to be in violation of international law. In addition, it is curious that France determines that cyber espionage is unacceptable when committed by states that it regards as its 'partners and allies'. One also needs to take with a pinch of salt China's condemnation of the NSA's activities given that only a few months before the Snowden revelations the Mandiant Report alleged that China is a persistent perpetrator of cyber espionage. However, the fact the Brazilian President cancelled a scheduled visit to Washington DC to meet the Obama administration, instead preferring to address the plenary body of the UN (the General Assembly), and in doing so carefully and purposively invoked unequivocal language in criticising the US's actions from an international law perspective, must be taken seriously when attempting to discern how the international community reflected upon the international legality of the NSA's conduct. The German position that the NSA's conduct was 'completely unacceptable' also implies condemnation of the NSA's conduct in every dimension (legal, political, ethical etc.) and can be reasonably construed as an international legal rebuke of the NSA's cyber espionage activities.

40 Ibid.

41 Quoted in 'Merkel Calls Obama about "US Spying on Her Phone"', *BBC News*, October 23, 2013, http://www.bbc.co.uk/news/world-us-canada-24647268.

42 Quoted in 'Hollande: Bugging Allegations Threaten EU-US Trade Pact,' *BBC News*, July 1, 2013, http://www.bbc.co.uk/news/world-us-canada-23125451.

43 Quoted in 'China Demands Halt to 'Unscrupulous' US Cyber-Spying,' *The Guardian*, May 27, 2014, http://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying.

44 Ibid.

45 See chapter 2 by Michael N. Schmitt and Liis Vihul, 44.

In this section I have argued that the principle of territorial sovereignty protects the territory of states from physical intrusion regardless of whether the intrusion produces damage. I have further argued that states exercise territorial sovereignty over cyber infrastructure that is physically located within their territory. As a result, I contend that acts of cyber espionage that intrude on the cyber infrastructure of a state for the purpose of intelligence-gathering constitute a violation of the principle of territorial sovereignty. I have alluded to recent examples of state practice in the context of cyber espionage to support this interpretation of international law.

4. The Principle of Non-Intervention

Cyberspace is used primarily as a domain for information communication. As such, it is possible that a state's confidential information may be intercepted as it is being transmitted through cyber infrastructure located on the territory of another state. In addition, since the emergence of cloud computing (and indeed its now widespread use), many states may even store confidential information in a central server that is located in the territory of another state. In such situations, although a state may assert ownership over the information that has been intercepted, there is no territorial basis on which it can claim a violation of its territorial sovereignty. Indeed, if information owned by one state (say the UK) is transmitted through the cyber infrastructure located on the territory of another state (say the US), and during transmission it is intercepted by another state (say France), it may be that the state on whose territory the cyber infrastructure is physically located (in my example, the US) will assert a violation of its territorial sovereignty. In such circumstances the principle of territorial sovereignty offers the state that has authored and thus asserts ownership over the information (the UK) very little protection. It is here that the principle of non-intervention becomes important.

Although sovereignty exhibits a strong territorial dimension '[a] State's power reaches beyond its territory'[46] and, in the words of the ICJ, protects its 'political integrity'[47] more generally. The non-intervention principle therefore represents international law's attempt to protect a state's sovereign right to determine its internal and external affairs free from external intervention.

The principle of non-intervention is firmly enshrined in international law. It is incorporated within numerous international (regional and bilateral) treaties[48] and, independent of these treaties, through their practice states have evidenced a clear view that

46 Benedict Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace,' in *Peacetime Regime*, Ziolkowski, 196.

47 'Between independent States, respect for territorial sovereignty is an essential foundation of international relations', and international law requires political integrity also to be respected'; Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 202, citing its judgment in The Corfu Channel Case, 35.

48 For a discussion see Maziar Jamnejad and Michael Wood, 'The Principle of Non-Intervention,' *Leiden Journal of International Law* 22 (2009): 362 *et seq*.

external intervention in their internal and external affairs is prohibited by way of customary international law. Consider, for example, the 1970 UN General Assembly's Friendly Relations Declaration, where the participating states acted with the purpose of giving expression to principles of a legal character and specifically declared that states are under a duty 'not to intervene in matters within the domestic jurisdiction of any State'.[49]

In 1986, the ICJ reiterated that the principle of non-intervention is 'part and parcel of customary international law'.[50] Clarifying the scope of the non-intervention principle, the ICJ explained:

> 'A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.'[51]

On the basis of this often quoted paragraph, the principle of non-intervention is generally distilled into two constitutive elements.[52] In order for an unlawful intervention to occur it must be established that: 1) the act committed intervenes in a state's sovereign affairs; and 2) that the act is coercive in nature. The application of these two elements to acts of cyber espionage against information which is being stored on or transmitted through cyber infrastructure located within the territory of another state will now be considered.

4.1 Sovereignty over Information Located outside State Territory

First and foremost, in order to establish an unlawful intervention the act in question must have a bearing upon matters which, by virtue of the principle of state sovereignty, a state is entitled to decide freely. The purpose of this criterion is to assess whether the alleged intervention pertains to a matter that is permissibly regulated by states on the basis that it falls within their sovereign authority, or whether states have instead determined through international law that it is a matter that falls outside of the realm of state sovereignty.

In the context of the current discussion, the important question is whether states exercise sovereignty over information that they have authored and compiled but which is stored on or being transmitted through cyber infrastructure located on the territory of another state.

In the mid-1960s the US began sending satellites into outer space in order to collect intelligence relating to the activities of other states. The principle of territorial

49 United Nations, General Assembly resolution 25/2625, *2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations*, A/RES/25/2625 (24 October 1970), http://www.un-documents.net/a25r2625.htm.

50 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 202.

51 Ibid, para. 205.

52 Jamnejad and Wood, 'The Principle of Non-Intervention,' 347.

sovereignty was not relevant because the surveillance was committed from outer space and no physical infraction of the victim state's territory was committed.[53] When the US used its satellites to collect information relating to the activities of the Soviet Union, the Soviet Union insisted that its sovereignty had been interfered with. In the words of the Soviet representative to the UN:

> 'The object to which illegal surveillance is directed constitutes *a secret guarded by a sovereign state*, and regardless of the means by which such an operation is carried out, it is in all cases an intrusion into something guarded by a sovereign state in conformity with its sovereign prerogative.'[54]

The recent *East Timor v Australia* litigation before the ICJ is also instructive here. East Timor alleged that Australia had sent its agents into the office of an Australian lawyer acting as legal counsel for East Timor to collect confidential information relating to existing litigation between the two states. The office was physically located in Australia. East Timor applied to the ICJ for a provisional order that declared '[t]hat the seizure by Australia of the documents and data violated (i) the sovereignty of Timor-Leste and that 'Australia must immediately return to the nominated representative of Timor-Leste and all of the aforesaid documents and data, and to destroy beyond recovery every copy of such documents and data that is in Australia's possession or control'.[55]

In addressing these requests, the ICJ noted that '[a]t this stage of proceedings, the Court is not called upon to determine definitively whether the rights which Timor-Leste wishes to see protected exist; it need only decide whether the rights claimed by Timor-Leste on the merits, and for which it is seeking protection, are plausible'.[56] Importantly, the ICJ did consider East Timor's claim 'plausible'[57] and granted a provisional order that 'Australia [must] not interfere in any way in communications between Timor-Leste and its legal advisers',[58] indicating that this conclusion 'might be derived from the principle of the sovereign equality of States, which is one of the fundamental principles of the international legal order and is reflected in Article 2, paragraph 1, of the Charter of the United Nations'.[59]

This was a provisional order of the ICJ and the Court did not definitively pronounce on the international legality of Australia's conduct. But this does not mean that the ICJ's interpretation of international law is without significance. Instead, I contend that the ICJ's reasoning is important because it suggests that although the

53 Richard A. Falk, 'Space Espionage and World Order: A Consideration of the Samos-Midas Program,' in *Essays on Espionage*, Falk.
54 Soviet Union Statement to the United Nations First Committee, quoted in Joseph Soraghan, 'Reconnaissance Satellites: Legal Characterisation and Possible Utilisation for Peacekeeping,' *McGill Law Journal* 13 (1967): 470-471 [my emphasis]. Although for a different view see 'Legal Aspects of Reconnaissance in Airspace and Outer Space,' *Columbia Law Review* 61 (1961): 1095 ('Thus it would seem that there are at present no principles of international law that prohibit reconnaissance from outer space').
55 Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), 147 Reports of Judgments (International Court of Justice 2014), para. 2.
56 Ibid, para. 26.
57 Ibid, para. 28.
58 Ibid, para. 55.
59 Questions Relating to the Seizure and Detention, para 27.

appropriated information was physically located in the office of East Timor's legal advisor in Australia, it was nevertheless plausible that the information was clothed with East Timorese sovereignty and intervention with that information was precluded by international law.

By analogy, I would argue that where a state stores confidential information in servers located in another state or transmits such information through cyber infrastructure located in another state, that information represents 'a crucial dimension of national sovereignty that presupposes the nation state' and the right to have that information protected from intrusion flows from the general entitlement of states to have their political integrity respected, that is their sovereignty.[60] The argument that information is integral to a state's sovereignty is particularly convincing where the information that has been intercepted relates to the exercise of a state's public functions. With regard to information relating to a state's commercial transactions, the argument that such information is protected by state sovereignty is harder to sustain.[61]

In support of this approach, Article 5 of the UN Convention on Jurisdictional Immunities of States and Their Property provides that '[a] State enjoys immunity, in respect of itself and its property, from the jurisdiction of the courts of another State'.[62] Article 10 explains however that a state cannot invoke its immunity in relation to proceedings arising out of a 'commercial transaction'. Read together, these provisions indicate that a state's sovereignty extends to its property (providing this property is used for exclusively non-commercial purposes) even when this property is physically located in the territory of another state and, as such, is considered inviolable. In light of these provisions, and specifically in the context of electronic information that a state has authored but which is located outside of its territory, von Heinegg argues that it is a 'general principle of public international law according to which objects owned by a State or used by that State for exclusively non-commercial purposes are an integral part of the State's sovereignty and are subject to the exclusive jurisdiction of that State'.[63] The upshot is that data which belongs to a state but which is being stored on or transmitted through cyber infrastructure located on the territory of another state possesses 'national data sovereignty' and interference with that data (for the purpose of espionage, for example) can be regarded as an intrusion into state sovereignty.[64]

4.2 Coercion and Cyber Espionage

Once it has been concluded that there has been intervention in a matter that falls within a state's *sovereign affairs*, in order to establish an unlawful intervention it must then be determined that the intervention is coercive in nature.

60 Kristina Irion, 'Government Cloud Computing and National Data Sovereignty,' *Policy and Internet* 4 (2012): 42.
61 Vineeth Narayanan, 'Harnessing the Cloud: International Law Implications of Cloud-Computing,' *Chicago Journal of International Law* 12 (2012): 783.
62 United Nations, General Assembly resolution 59/38, *United Nations Convention on Jurisdictional Immunities of States and Their Property*, A/RES/59/38 (2 December 2004), http://legal.un.org/ilc/texts/instruments/english/conventions/4_1_2004_resolution.pdf.
63 Von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' 130.
64 Irion, 'Government Cloud Computing and National Data Sovereignty.'

The leading authority on the meaning of coercion is the *Nicaragua* judgement. In this case the ICJ defined coercion as acts interfering with 'decisions' and 'choices' of the victim state in relation to matters falling within its sovereignty. Following on from this decision there seems to be near consensus within academic literature that coercion requires the imposition of 'imperative pressure'[65] which manipulates the will of the state in order for the entity exercising coercion to realise certain objectives or, in Oppenheim's famous and often quoted formulation, intervention is 'dictatorial interference … in the affairs of another State for the purpose of maintaining or altering the actual condition of things'.[66] For Jamnejad and Wood, coercion is imposed where 'action is taken by one state to secure a change in the policies of another'.[67] In this sense, the dividing line between permissible influence and impermissible intervention in sovereign affairs is whether the act in question compels the state to act, or to abstain from acting, in a manner that it would not have voluntarily chosen.

This interpretation may be readily fulfilled in many cases of malicious cyber conduct. Take for example the Distributed Denial of Service Attacks against Estonia in 2007, a series of cyber attacks which impaired the Estonian government's capacity to freely communicate and interact with domestic and international actors.[68] However, an interpretation of coercion that requires the imposition of pressure yields important consequences for the application of the non-intervention principle to cyber espionage. This is because cyber espionage describes the practice of accessing and obtaining confidential information and, provided confidential information is accessed and obtained, cyber espionage is committed regardless of how that information is subsequently used.[69] Thus, in and by itself cyber espionage does not entail the imposition of pressure upon a state. Consequently, an interpretation of coercion that requires the imposition of pressure would mean that cyber espionage cannot be considered coercive and therefore does not violate the principle of non-intervention. For Ziolkowski:

> 'A forbidden intervention in domestic affairs requires an element of coercion by the other state. Scholars assert that illegal coercion implies massive influence, inducing the affected state to adopt a decision with regard to its policy or practice which it would not entertain as a free and sovereign state. It is clear that clandestine information gathering as such will not fulfil such requirements.'[70]

65 William Michael Reisman, *Nullity and Revision: The Review and Enforcement of International Judgments and Awards* (New Heaven: Yale University Press, 1971), 839-40.

66 Lassa Oppenheim and Hersch Lauterpacht, *International Law: A Treatise. Vol. I, Peace*, 8th edn (London: Longman, 1955), 305.

67 Jamnejad and Wood, 'The Principle of Non-Intervention,' 347-348.

68 For a discussion of the impact that the DDOS attacks had on Estonia see The North Atlantic Treaty Organization, *Six Colours: War in Cyberspace*, 2013, http://www.nato.int/ebookshop/video/six_colours/SixColours.html. On the application of international law to this event see Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' *Journal of Conflict and Security Law* 17 (2012): 211.

69 Where information obtained as a result of cyber espionage is subsequently used to exert influence over the victim state, a violation of the non-intervention is likely to occur. However, an examination of the international legality of this type of conduct falls outside of the scope of this chapter.

70 Ziolkowski, 'Peacetime Cyber Espionage,' 433. For a similar view see Terry Gill, 'Non-Intervention in the Cyber Context,' in *Peacetime Regime*, Ziolkowski, 224 ('the obtaining of information in itself falls short of coercive or dictatorial interference, and would not constitute 'intervention' in the legal sense').

I argue that this is a particularly narrow interpretation of the concept of coercion and which is undesirable as a matter of policy and incorrect as a matter of law. In normative terms this narrow interpretation is undesirable because, as I have already noted, the principle of sovereignty is a constitutional norm of international relations and, as such, requires robust protection. As we have seen, the principle of territorial sovereignty is defined broadly in order to provide watertight protection to the territorial dimension of state sovereignty – any intrusion into a state's sovereign territory is prohibited. The principle of non-intervention is also designed to protect a state's sovereignty, but this principle protects the metaphysical aspect of sovereignty (a state's political integrity) rather than its physical dimension (a state's territory). However, if a state's political integrity is protected only where the state is subject to imperative pressure (and especially 'massive influence'), then a state's political integrity is inadequately protected. In order to ensure that the depth and breadth of the legal principle of non-intervention accords with the depth and breadth of the constitutional norm of state sovereignty, I argue that conduct which compromises or undermines the authority of the state should be regarded as coercive.

This broader reading of the term coercion finds support within academic commentary. McDougal and Feliciano argue that a finding of coercion can be made whenever there is an attack against the 'value' of sovereignty.[71] My approach also chimes with Dickinson's claim that coercion is present if 'intervention cannot be terminated at the pleasure of the state that is subject to the intervention'.[72]

This expansive understanding of coercion also finds support in state practice and the practice of international organisations, notably the UN General Assembly. The 1965 UN Declaration on the Inadmissibility of Intervention and the 1970 Friendly Relations Declaration employ identical language in articulating the scope of the non-intervention principle, explaining that no state has 'the right to intervene, directly or indirectly, for any reason whatever, in sovereignty of any other State' or use 'any … measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights'. As is apparent, in these Declarations the principle of non-intervention is formulated in particularly broad terms and they seem intended to encourage an expansive reading of the prohibition against intervention: 'for whatever reason'; 'any measures'; 'to obtain from it the subordination of the exercise of its sovereign rights'.

Additional support for this broader reading of the non-intervention principle is evident from the reaction of the Soviet Union to the US's exploitation of outer space for purpose of unauthorised surveillance in the 1960s, discussed above. Even in the absence of a violation of its territorial sovereignty the Soviet Union asserted that the US's conduct constituted a violation of its political integrity and in making this

71 Myres Smith McDougal and Florentino P. Feliciano, 'International Coercion and World Public Order: The General Principles of the Law of War,' *The Yale Law Journal* 67 (1958): 782.

72 Edwin De Witt Dickinson, *The Equality of States in International Law* (Cambridge, Mass.: Harvard University Press, 1920), 260.

determination explained that 'in all cases an intrusion into something guarded by a sovereign state in conformity with its sovereign prerogative' is unlawful.[73]

Further support for this expansive interpretation of the concept of coercion is found in the recent *East Timor v Australia* litigation. In this case the ICJ granted a provisional order on the basis that it was plausible that Australia's interception of information belonging to East Timor but located on Australian territory constituted a violation of East Timor's sovereignty; namely, a prohibited intervention. Importantly, it was the *impact* of Australia's conduct on East Timor's sovereignty that implied a violation of international law, independent of any attempt by Australia to subsequently use that appropriated information to compel East Timor into acting in one way or another.

The most sustained judicial consideration of the non-intervention principle is the ICJ's judgment in *Nicaragua* and this decision contends that coercion is present only where a state's decision making capacity is affected. However, it is important not to overstate the significance of the ICJ's interpretation of the non-intervention principle. As the ICJ questioned in this case, 'what is the exact content of the [non-intervention] principle so accepted'?[74] In addressing this question the ICJ specifically noted that 'the Court will define only those aspects of the principle which appear to be relevant to the resolution of the dispute'.[75] This is important because the ICJ explained that the specific non-use of force prohibition can be considered an aspect of the general non-intervention principle (the ICJ noted that intervention is 'particularly obvious in the case of intervention which uses force')[76] and the ICJ's immediate focus in this case was the prohibition against the use of force. After noting that Nicaragua's complaints against the US related mainly to its military activities, the ICJ explained that 'it is primarily acts of intervention of this kind with which the Court is concerned in the present case'.[77] Consequently, the ICJ's decision in *Nicaragua* can be read as providing an inchoate or even unfinished delineation of the non-intervention principle and if this is correct then this decision is of little relevance to determining whether conduct not involving the use of force (such as cyber espionage) offends the prohibition against intervention.

All in all, I argue that there is no requirement that influence (let alone massive influence) be imposed upon a state to pursue a particular course of action, or indeed to abstain from one, in order to constitute coercion and thus fall foul of the non-intervention principle. Instead, the key issue is whether the conduct in question compromises or undermines the authority structures of the state, that is, state sovereignty. With reference to cyber espionage, I have already demonstrated that states exercise 'national data sovereignty' over information that they have authored and compiled, even when it is physically located on the cyber infrastructure of another state. In light

73 Soviet Statement in the United Nations First Committee, quoted in Soraghan, 'Reconnaissance Satellites,' 470-471.
74 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 205.
75 Ibid.
76 Ibid.
77 Ibid.

of this, where such data is accessed and appropriated the sovereign authority of the state is compromised and the conduct in question can be regarded as coercive.

Some may express concern that this interpretation of the concept of coercion is overly broad and casts the scope of the non-intervention principle far too widely. In particular, the concern may be that such an expansive interpretation would essentially confer on states an international legal entitlement to operate unaffected by the conduct and activities of other states. Clearly, such an approach does not accord with international reality. Given the pressures of globalisation, and in light of the intensity of state interactions in contemporary international relations, it is clear that a reading of the non-intervention principle which more or less precludes intensive state interactions on the basis that this results in their sovereignty being undermined is incorrect as a matter of international law. To put the same matter differently, states are constantly interacting in order to pursue and realise their particular interests and such interactions frequently result in the sovereignty of other states being undermined, yet states rarely denounce each and every act that impacts upon their sovereignty as unlawful intervention.

In this regard it needs to be remembered that the application of the non-intervention prohibition is subject to the principle of *de minimis non curat lex* – which is generally translated from Latin as *the law does not concern itself with trifles*. The effect of the *de minimis* doctrine is to place 'outside the scope of legal relief the sorts of intangible injuries, normally small and invariably difficult to measure, that must be accepted as the price of living in society'.[78] Thus, this maxim signifies 'that mere trifles and technicalities must yield to practical common sense and substantial justice' so as 'to prevent expensive and mischievous litigation, which can result in no real benefit to the complainant, but which may occasion delay and injury to other suitors'.[79]

Although often described as a maxim, this principle does impose a recognised legal restriction on the operation of the non-intervention principle.[80] McDougal and Feliciano suggest that determining coercion should account for 'consequentiality'.[81] They suggest 'the importance and number of values affected, the extent to which such values are affected, and the number of participants whose values are so affected'.[82] In the context of cyber, Watts argues that when applying the *de minimis* threshold to the non-intervention principle our understanding of the term coercion should include a consideration of 'the nature of State interests affected by a cyber operation, the scale of the effects the operation produces in the target State, and the reach in terms of number of actors affected'.[83] After taking such considerations into account, acts which have an insignificant impact upon the authority structures of a sovereign state (those

78 Jeff Nemerofsky, 'What is a "Trifle" Anyway?' *Gonzaga Law Review* 37 (2001-2002): 323.
79 Ibid.
80 Robert Jennings and Adam Watts, eds., *Oppenheim's International Law* (Longman, 1996) 385 *et seq*; Rosalyn Higgins, 'Intervention and International Law,' in *Intervention in World Politics*, ed. Hedley Bull (Clarendon Press, 1984), 30; Watts, 'Low-Intensity Cyber Operations,' 138.
81 McDougal and Feliciano, 'International Coercion and World Public Order: The General Principles of the Law of War,' 782.
82 Ibid.
83 Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' 146.

that cause mere irritation or inconvenience) do not warrant the application of international law and thus do not violate the non-intervention principle.

With regard to cyber espionage specifically, much will depend upon the facts of the case in question, and in particular the extent to which the cyber espionage compromises the sovereign authority of the state. Primarily, this will require an assessment of the scale of the cyber espionage under examination and an analysis of the nature of the information that has been appropriated. For the purpose of illustration, it can perhaps be contended that whilst the systematic accessing of information belonging to senior state officials (such as the Head of State) is likely to exceed the *de minimis* threshold, the one-off accessing of innocuous electronic correspondence of a low-ranking civil servant is unlikely to be considered sufficiently serious to justify the engagement of international law.

5. Is There a Customary Defence of Cyber Espionage?

In the context of espionage a frequently made argument is that even if espionage does constitute a *prima facie* violation of the principle of territorial sovereignty or the non-intervention principle, state practice has established a customary international law that modifies the scope of the these principles. In other words, state practice has given rise to a permissive rule of customary international law that regards espionage as a legally recognised exception to the principles of territorial sovereignty and non-intervention. In the words of Smith:

> 'Because espionage is such a fixture of international affairs, it is fair to say that the practice of states recognises espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law.'[84]

The claim that is frequently advanced is that, if espionage is permissible under customary international law, espionage committed through cyberspace must also be permissible.[85] Several important observations need to be considered here.

Customary international law emerges on the basis of 'general practice accepted as law'.[86] There are thus two elements of customary international law.[87] First, state

84 Jeffrey H. Smith, 'State Intelligence Gathering and International Law: Keynote Address,' *Michigan Journal of International Law* 28 (2007): 544. Similarly, see Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law,' *Michigan Journal of International Law* 28 (2007): 628 ('[s]tate practice throughout history … supports the legitimacy of spying. Nowhere in international law is peaceful espionage prohibited').

85 Gary Brown and Keira Poellet, 'The Customary International Law of Cyberspace,' *Strategic Studies Quarterly* 6 (2012): 133; Fidler, 'Economic Cyber Espionage.'

86 United Nations, *Statute of the International Court of Justice*, Article 38(1)(b).

87 '[F]or a new customary rule to be formed, not only must the acts concerned amount to a settled practice, but they must be accompanied by the *opinio juris sive necessitatis*'; Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 207.

practice; and second, the requirement that this practice is accompanied by a belief that it is permitted under international law (*opinio juris*). The burden is on those asserting the existence of customary rule to demonstrate that these two criteria are met.

In relation to state practice, in the *North Sea Continental Shelf Cases* the ICJ explained that in order to find that a customary rule has emerged there must be 'extensive and virtually uniform' state practice in favour of that rule.[88] Although this does not require universal acceptance of that rule by states within the international community or even that those states which practice the rule do so with strict conformity,[89] this is nevertheless an extremely high threshold. This notwithstanding, those advocating the existence of a customary rule permitting espionage confidently assert that most states most of the time collect confidential intelligence without authorisation from other states (that is, they commit espionage) and thus this stringent threshold is attained.

However, in order to qualify as state practice it must be conducted publically and openly and state practice committed in secret is irrelevant to the formation of customary international law.[90] In relation to state practice committed in secret, the International Law Commission's Second Report on the Identification of Customary International Law explains that '[i]t is difficult to see how [such] practice can contribute to the formation or identification of general customary international law'.[91] The requirement that state practice be committed publically and openly is important because states must be given the opportunity 'to respond to it positively or negatively', so that they can either make the decision to adopt the rule, and thus further contribute to its formation, or instead reject it and attempt to frustrate its crystallisation;[92] or, if it appears that a state is isolated in its rejection of the rule, it can identify itself as a persistent objector to that rule. Patently, this process cannot occur where state practice is committed in secret. Furthermore, it seems inherent to the notion of the rule of law that binding rules are public in character and it is for this reason that the UN Charter forbids the use of secret treaties.[93]

Almost by definition, espionage is a practice conducted in secret. As a result, regardless of how frequently states engage in espionage, where this practice is engaged in covertly and secretly it cannot be classified as state practice for the purpose of customary law formation. In the context of espionage, the International Law Association's Committee on the Formation of Customary International Law

88 North Sea Continental Shelf Cases (Federal Republic of Germany/Denmark v. Federal Republic of Germany/Netherlands) 4 Reports of Judgments (International Court of Justice 1969), para. 74.

89 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 186.

90 United Nations, General Assembly, International Law Commissions, *Second Report on the Identification of Customary International Law*, A/CN.4/672, para. 47 (22 May 2014), http://legal.un.org/ilc/documentation/english/a_cn4_672.pdf.

91 Ibid.

92 'Another condition for State conduct – if it is to count in assessing the formation of custom – is that it must be transparent, so as to enable other States to respond to it positively or negatively'; Yoram Dinstein, 'The Interaction between Customary Law and Treaties,' *Recueil des Cours Recueil des cours* 322 (2006): 275.

93 United Nations, *Charter of the United Nations*, Article 102.

explains that 'a secret physical act (e.g. secretly 'bugging' diplomatic premises) is probably not an example of the objective element [of state practice]'.[94]

It is correct that in more recent times some states have been prepared to acknowledge *prospectively* that their security services engage in covert operations for the purpose of intelligence-gathering. For example, the Mission Statement of the US Central Intelligence Agency (CIA) explains that one of its objectives is to '[p] reempt threats and further US national security objectives by collecting intelligence that matters, producing objective all-source analysis, conducting effective covert action as directed by the President, and safeguarding the secrets that help keep our Nation safe'.[95] It is well accepted that verbal acts such as these can constitute state practice for the purpose of customary law formation.[96] Fundamentally, however, it must be remembered that customary international law forms on the basis of specific 'instances of State conduct'[97] that form 'a web of precedents'[98] from which an observable pattern is identifiable. Notwithstanding the broad public statements of the CIA relating to covert intelligence-gathering, it nevertheless remains that specific instances of espionage are committed in secret and to accept such conduct as evidence of state practice is at odds with the basic tenet of customary international law that state practice is 'material and detectable'.[99]

Even if we momentarily concede that there is sufficient evidence of state practice of espionage to satisfy the first limb of the customary international law test, in order for custom to form this practice must be accompanied by *opinio juris*; state practice alone, regardless of how widespread and systematic it is, is insufficient. The requirement is that when participating in a particular practice states must assert the international legality of their conduct or, at the very least, when the international legality of their conduct is challenged subsequent to its practice it can be defended on the basis that it is permissible under international law. This is hugely problematic in the context of espionage because when practising this type of activity states do not generally express the belief that it is permissible under international law. Furthermore, when challenged about their espionage activities, states overwhelmingly refuse to admit responsibility for this conduct, let alone attempt to justify it as permissible under international law. In the wake of the Snowden revelations President Obama did attempt to defend the NSA's conduct, but crucially he consistently defended the conduct on the basis that it was necessary to maintain 'national security'.[100] Conspic-

94 'Final Report of the Committee: Statement of Principles Applicable to the Formation of General Customary International Law' (Final Report of the Committee, International Law Association, London conference, 2000), 15.

95 Central Intelligence Agency, 'CIA Vision, Mission, Ethos & Challenges,' https://www.cia.gov/about-cia/cia-vision-mission-values.

96 United Nations, General Assembly, International Law Commissions, *Second Report on the Identification*, para. 37.

97 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 184.

98 Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain), 3 Reports of Judgments (International Court of Justice 1970), para. 39 (Separate Opinion of Judge Ammoun).

99 François Gény, 'Méthode d´interprétation et sources en droit privé positif,' *A. Chevalier-Marescq* 1 (1899): section 110, quoted in Anthony A. D´Amato, *The Concept of Custom in International Law* (Ithaca N.Y. and London: Cornell University Press, 1971), 49.

100 The White House, Office of the Press Secretary, *Remarks by the President on Review of Signals Intelligence*, 17 January 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

uously absent from President Obama's defence was that the conduct was permissible under *international law*, and the requirement of *opinio juris* is only satisfied where the conduct in question is justified as acceptable under international law.

It would therefore appear that state practice of espionage 'is accompanied not by a sense of right but by a sense of wrong'[101] and so 'state practice and *opinio juris* appear to run in opposite directions'.[102]

A further point is relevant here. When states discover that they are the victims of espionage they often protest (and often vociferously) that such conduct is contrary to international law. When a customary rule is in the process of formation and a number of states of the international community object to that rule on the basis that it is incompatible with international law, it becomes particularly difficult to sustain the claim that a customary rule has formed – in essence, a common *opinio juris* forms agitating against the emergence of a customary rule.[103] This point is particularly relevant in relation to cyber espionage. If we look at the international reaction to the Snowden revelations we see a cohort of states asserting that the NSA's practice of cyber espionage was incompatible with international law. As we have already seen, Germany and Brazil in particular objected to the NSA's cyber espionage and in doing so clearly employed the language of international law; indeed, Brazil advocated its international law objections before the UN General Assembly.

The events surrounding Sony in late 2014 are also illustrative. As is well known, Sony intended to release a film entitled *The Interview* which depicted the assassination of the leader of North Korea. Days before its release Sony's computer networks were accessed without authorisation and malware was introduced which wiped a substantial amount of confidential information. In addition, certain confidential information was exfiltrated and published on the Internet, including sensitive email correspondence between the company and its employees (well-known actors) and storylines for forthcoming films.[104]

The US Federal Bureau of Investigation (FBI) determined that North Korea was responsible for this malicious cyber conduct.[105] Although the US did not specify on what basis this conduct constituted a violation of international law, the US explained that it would 'respond proportionally and in a space, time and manner that we choose'.[106] Indeed, on 2 January 2015 the US imposed economic sanctions against North Korea, including freezing its assets in the US.[107] As we know, under international law a state that is subject to an internationally wrongful act is entitled

101 Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs,' 17.
102 Simon Chesterman, 'The Spy Who Came in from the Cold: Intelligence and International Law,' *Michigan Journal of International Law* 27 (2006): 1072.
103 Frederic L. Kirgis, Jr., 'Custom on a Sliding Scale,' *American Journal of International Law* 81 (1987): 146.
104 For an overview of the events see 'The Interview: A Guide to the Cyber Attack on Hollywood,' *BBC News*, December 29, 2014, http://www.bbc.co.uk/news/entertainment-arts-30512032.
105 'Sony Hack: Obama Vows Response as FBI Blames North Korea,' *BBC News*, December 19, 2014, http://www.bbc.co.uk/news/world-us-canada-30555997.
106 Ibid.
107 Dan Roberts, 'Obama Imposes New Sanctions against North Korea in Response to Sony Hack,' *The Guardian*, January 2, 2015, http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.

(subject to caveats) to adopt proportionate countermeasures in order to compel the wrongdoing state to discontinue its internationally wrongful conduct and make appropriate reparations. The only implication, then, is that the US regarded this malicious cyber conduct as incompatible with international law.

For the purpose of this article, which discusses the international legality of cyber espionage, we must approach cautiously the US's determination that this cyber conduct was unlawful under international law. This is because when determining that the malicious cyber conduct was unlawful the US seemed to refer to the incident as a whole and not specifically to those aspects of the malicious cyber conduct that constituted cyber espionage. It is therefore unclear as to whether the US's protest was in relation to the hacking of cyber infrastructure located on its territory, the emplacement of malware that erased data located on cyber infrastructure located on its territory, or the exfiltration of confidential data located on cyber infrastructure located on its territory, or all three. However, given that the cyber espionage dimension of the incident was by far the most pronounced, a reasonable reading of the US's reaction to the Sony incident is that it regarded such conduct as incompatible with international law. If this reading is correct, it would lend further support to the argument that 'there is little doctrinal support for a 'customary' defence of peacetime espionage in international law'.[108]

6. Conclusion

This chapter does not deny the importance of intelligence-gathering in the contemporary world order. However, one must distinguish between intelligence-gathering from publically available sources and intelligence-gathering from private, unauthorised sources, namely espionage. 'Intelligence gathering that relies upon open source information is legally unproblematic'.[109] One must also distinguish between authorised and unauthorised intelligence-gathering. Intelligence that is gathered pursuant to a treaty regime or Chapter VII Security Council Resolution, for example, can be regarded as authorised, and for this reason is not properly regarded as espionage. This chapter has examined the international legality of transboundary state-sponsored cyber espionage and has argued that cyber espionage constitutes a violation of the territorial sovereignty of a state where information is accessed that is resident on computer networks that are supported by cyber infrastructure located on that state's territory. I have identified recent state practice which supports this conclusion. I have also argued that cyber espionage violates the principle of

108 Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection,' *Journal of National Security Law and Policy* 5 (2011): 203.

109 Chesterman, 'The Spy Who Came in from the Cold: Intelligence and International Law,' 1073.

non-intervention where it has a more than insignificant impact on the authority structures of a state. The utility of the non-intervention principle is particularly apparent in relation to information that belongs to a state but is located on cyber infrastructure in the territory of another state. Finally, I have argued that customary international law develops on the basis of transparent, publically observable state conduct that is committed in the belief that it is permissible under international law. As espionage is a practice that is by definition committed in secret, and where states overwhelmingly refuse to admit responsibility for such conduct let alone justify it as acceptable under international law, I have concluded that there is no customary 'espionage exception' to the principles of territorial sovereignty and non-intervention.

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

CHAPTER 5

Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace

Toni Erskine and Madeline Carr[1]

As in any realm of human activity, norms are unavoidable in cyberspace. Yet cyberspace is a singularly complex setting within which to understand and try to shape norms. The problem is not simply the nature of cyberspace, although, as we will address below, acknowledging the unique characteristics of cyberspace is crucial when exploring norms in this realm. Rather, the challenge lies in the often overlooked *nature of norms themselves* and how their defining features render them especially difficult to decipher – and, by extension, to attempt to design – in the context of cyberspace.

Norms are widely-accepted and internalised principles or codes of conduct that indicate what is deemed to be permitted, prohibited, or required of agents within a specific community. The modest aim of our chapter is to explore the challenges and potential of engaging with norms in cyberspace. By 'engaging with norms in cyberspace' we mean both *understanding existing norms* and the more prominent endeavour (prevalent in recent discussions of policies related to both cyber security and Internet governance) of what is variously described as *'cultivating', 'promoting'*

1 An initial iteration of this position was presented at the NATO CCD COE workshop on 'Cyber Norms & International Relations' in Stockholm, Sweden, 28-29 April 2014. We are grateful to Anna-Maria Osula and Henry Rõigas for the opportunity to develop our argument for this volume, to Nicholas Erskine, Nishank Motwani, Cian O'Driscoll and anonymous reviewers for their incisive written comments on an earlier draft, and to Campbell Craig for discussing particular points.

or *'developing' new norms.*[2] Our focus throughout most of this chapter will be on the former. Indeed, a central point of the argument that will follow is that one cannot hope to 'cultivate' norms in cyberspace without first understanding the existing normative landscape.

In order to explore the challenges and potential of engaging with norms in cyberspace, we will take five steps. First, we will elaborate upon the definition of 'norms' offered above. In doing this, we will draw on influential work from within the discipline of International Relations (IR), and specifically from the multifaceted approaches labelled 'normative IR theory' and 'constructivism'.[3] Second, we will introduce a task that is fundamental to understanding existing norms in any realm, including cyberspace: interpreting the norms themselves. Third, we will highlight the characteristics of cyberspace that render this crucial task particularly difficult; namely, that it is a new and rapidly changing realm in which underlying values are contested and relevant agents are often difficult to identify. Fourth, we will link the difficulties of addressing norms in such a realm with the tendency to invoke what we will call 'quasi-norms', or merely *purported* norms. Fifth and finally, we will turn to the potential to engage with norms in cyberspace, regardless of obstacles, by uncovering what we will call the 'norm of de-territorialised data' and, in the process, demonstrating how evidence for its status as such can be uncovered in the justifications and judgements that agents in international politics offer when it is violated. Our hope is that these preliminary steps will take us some distance towards establishing a conceptual framework for speaking more coherently about norms in cyberspace.

2 'Cultivating' is a term used by Martha Finnemore in 'Cultivating International Cyber Norms', in *America's Cyber Future: Security and Prosperity in the Information Age*, eds. Kristin M. Lord and Travis Sharp (Washington, D.C.: Center for a New American Security, 2011), 89-101, https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf. (She also employs 'formulating' and 'implementing' seemingly synonymously at page 99, which, for reasons that we will try to make clear below, is more problematic.). 'Promoting' is employed by, *inter alia,* Henry Farrell, 'Promoting Norms for Cyberspace,' *Council on Foreign Relations*, April 2015, 1-3, http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358. A series of workshops jointly held by Harvard, MIT and University of Toronto discussed 'developing' cyber norms. American Bar Association, 'A Call to Cyber Norms: Discussions at the Harvard-MIT-University of Toronto Cyber Norms Workshops, 2011 and 2012' (2015), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2015apr14_acalltocybernorms.authcheckdam.pdf.

3 For an overview of 'normative IR theory' (which is also referred to as 'international political theory' and 'international ethics'), see Toni Erskine, 'Normative International Relations Theory,' in *International Relations Theory: Discipline and Diversity,* eds. Tim Dunne, Milja Kurki and Steve Smith (Oxford: Oxford University Press, 2nd ed. 2010 and 4th ed. 2016), 236-258. For a general introduction to IR's 'constructivism', see Ian Hurd, 'Constructivism,' in *The Oxford Handbook of International Relations,* eds. Christian Reus-Smit and Duncan Snidal (Oxford: Oxford University Press, 2008), 298-316. For an essay that compares and contrasts these bodies of scholarship, see Toni Erskine, 'Whose Progress, Which Morals? Constructivism, Normative IR Theory and the Limits and Possibilities of Studying Ethics in World Politics,' *International Theory* 4 (2012).

1. Defining 'Norms': Insights from the Discipline of International Relations

In early 2015, Admiral Michael S. Rogers, head of the National Security Agency (NSA) and Cyber Command in the United States (US) announced his intention to 'do outreach in the academic world' in order to better understand norms in cyberspace. In making the case for 'a strong academic focus' in addressing norms in the cyber context, and comparing this current challenge to 'another cataclysmic change in national security in the middle of the previous century', namely the advent of the nuclear age, he noted that work that led to understanding and fostering 'established norms of behaviour' in relation to nuclear weapons, such as those surrounding deterrence, was 'done in the academic arena'.[4] Although Admiral Rogers did not elaborate on the precise source of this work, it seems clear that he was inclined in his outreach efforts to look particularly to the discipline of IR, within which prominent works on the political, ethical, psychological and security aspects of nuclear weapons and deterrence theory are found.[5] We will respond to Rogers' call for engagement with the academic community, and particularly with the discipline of IR, by suggesting that normative IR theory and constructivism, both relatively recently-established areas of scholarship within the discipline, are valuable places to begin acquiring the necessary conceptual tools for addressing the subject of norms in cyberspace.

Contributions to normative IR theory and what we will call 'mainstream constructivism' have engaged in separate analyses of norms, with distinct research aims and methodologies.[6] Nevertheless, they adopt valuable, shared assumptions about their common object of analyses. A 'norm' as it is generally understood within these IR approaches – and as we will use the term here – is a principle that displays two

4 Michael S. Rogers, 'A Conversation with Mike Rogers,' *Cyber Security for a New America: Big Ideas and New Voices*, February 23, 2015, https://www.newamerica.org/new-america/cybersecurity-for-a-new-america/.

5 This body of work has spanned IR's security studies, political realism, (early) normative IR theory, and, more recently, constructivism. Prominent works in security studies include, Thomas C. Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960 and 1980); Robert Jervis, Richard Ned Lebow and Janice Gross Stein (with contributions by Patrick M. Morgan and Jack L. Snyder), *The Psychology of Deterrence* (Baltimore: Johns Hopkins University Press, 1985); Daniel Deudney, 'Nuclear Weapons and the Waning of the Real-State', *Daedalus,* 124: 2 (Spring 1995), 209-231; and Lawrence Freedman, *Deterrence*, 1st ed. (Cambridge: Polity, 2004). For an overview of American realist engagement with nuclear weapons and the problem of deterrence, see Campbell Craig, *Glimmer of a New Leviathan: Total War in the Realism of Niebuhr, Morgenthau, and Waltz* (New York: Columbia University Press, 2003) and 'The Nuclear Revolution as Theory,' in *International Relations Theory Today,* 2nd ed., eds. Ken Booth and Toni Erskine (Cambridge: Polity Press, 2016). Prominent neo-realist contributions are the following: Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca: Cornell University Press, 1985) and *The Meaning of the Nuclear Revolution: Statecraft and Prospects for Armageddon* (Ithaca: Cornell University Press, 1990); and Kenneth N. Waltz, 'Nuclear Myths and Political Realities', *American Political Science Review,* 84: 3 (Sept. 1990), 730-745. Influential precursors to normative IR theory on this topic are Paul Ramsey, *The Just War: Force and Political Responsibility* (Oxford; New York: Rowman and Littlefield, 1968 and 2002), Part III, and Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 1977 and 2nd ed. 1992), chapter 17. For a prominent constructivist study, see Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945* (New York: Cambridge University Press, 2007).

6 'Constructivism' within IR has various, multifaceted strands and we realise that a distinction such as that between 'mainstream' or 'empirical' constructivism on the one hand and 'critical' or 'language-based' constructivism on the other oversimplifies a sophisticated and diverse body of work. Our aim here is simply to make clear that our intended focus is the work of those empirically-minded constructivists, with firm roots in American IR, whose social scientific commitments have been amenable to mainstream IR, and who, collectively, have produced a significant body of work on norm development in international relations.

related, key characteristics: 1) it has prescriptive and evaluative force; and 2) it is widely-accepted and internalised by those within a particular community.

Norms as phenomena studied in IR are principles that embody established codes of what actors *should* do, or refrain from doing, in certain circumstances. Thus conceived, they possess prescriptive force. By extension, norms also entail an evaluative dimension: norms are invoked to variously condemn or condone behaviour in world politics, and even to support proposals for sanctions when they have been violated. In short, they embody powerful expectations that can both constrain and compel actors in world politics. As guides to what is required, permitted, or prohibited, they are widely understood to have moral weight.[7] To highlight this important feature of norms, they have been referred to as 'moral norms' within both mainstream constructivism and normative IR theory.[8] This label highlights their important prescriptive and evaluative dimension. Moreover, it distinguishes this conception of a norm both from its more colloquial counterpart, which simply connotes habitual behaviour ('it is the norm to break for coffee at 10am'), and from the broader category of 'social norms' which, Nina Tannenwald usefully notes, encompasses 'moral norms', but also includes 'more mundane kinds of norms or rules for social interaction, such as diplomatic protocol'.[9] Throughout this chapter, when we talk about 'norms' in cyberspace, or in international relations more generally, we will be referring to norms that can be thus labelled.

Both broadly communitarian positions within normative IR theory and IR's constructivism see norms as social facts that are intersubjectively defined.[10] Simply, shared understandings regarding right and wrong conduct are established over time by those who participate in particular practices. (We understand practices as sustained interactions between purposive actors that both rely on and establish rules, customs, and common meanings.) Norms are principles that represent these collective expectations and are both widely accepted and internalised by the members of the community within which they evolve. Importantly, the community in question need not be territorially defined, but can emerge in the context of geographically dispersed and often transnational practices.[11] Norms might be codified in law, or

7 Erskine, 'Normative International Relations Theory,' 246-247.

8 See, for example, Richard Price, 'The Ethics of Constructivism,' in *The Oxford Handbook of International Relations,* eds. Reus-Smit and Snidal, 317-326 and Erskine, 'Normative International Relations Theory.'

9 Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945,* 58. Notably, we do not agree with Tannenwald's account that 'moral norms' are necessarily 'rooted in impartiality' and are 'universalisable' in the Kantian sense. Moral norms as we understand them can also boast a particularist moral starting point and be circumscribed in scope.

10 For an account of the common ground between communitarian normative IR theory and IR's constructivism, see Erskine, 'Whose Progress, Which Morals?' 462-463. Emmanuel Adler provides and incisive account of intersubjectivity in Emanuel Adler, 'Seizing the Middle Ground: Constructivism in World Politics,' *European Journal of International Relations* 3 (1997): 327-328. The seminal work in establishing a broad analytical distinction between 'communitarianism' and 'cosmopolitanism' in normative IR theory is Chris Brown, *International Relations Theory Today: New Normative Approaches* (New York: Columbia University Press, 1992). The broadly 'communitarian' theorists central to work in normative IR theory whose understanding of norms we are relying on here are Michael Walzer and Mervyn Frost, both of whom will be addressed below.

11 For a detailed account of this conception of 'dislocated community' (that addresses 'morally constitutive communities' but also applies to communities of shared understandings and emerging norms), see Toni Erskine, *Embedded Cosmopolitanism: Duties to Strangers and Enemies in a World of Dislocated Communities* (New York: Oxford University Press, 2008), 173-174; 218-227. This understanding of community as not necessarily territorially defined is important when we are talking about norms in cyberspace.

they might be internalised *without* being formally institutionalised. Either way, their defining feature is that they are widely accepted by, and inform the behaviour of, those who participate in the relevant practice. By this account, it is conceivable that a law might *not* constitute a norm if it is neither internalised by, nor informs the behaviour of, those to whom it is meant to apply.[12] Indeed, while a principle might be widely accepted and internalised within a community (in other words, achieve the status of a norm) *before* being codified in law, it is also the case that formally institutionalising a principle in law may contribute to its eventual (but not inevitable) acceptance as a norm. Our point here is simply that laws and norms are often overlapping categories, but they are not equivalent. In sum, norms embody a community's widely accepted and internalised customs, mores and perceived rules regarding right and wrong conduct in relation to particular practices.

The norms that are subjects of study in IR are typically those associated with international practices, by which we mean, simply, practices whose participants – whether individual human beings or corporate agents – are not restricted to those within the borders of any one state. The category of *international* norm that we associate with such practices might elicit scepticism. It suggests the possibility of agreement on expectations and standards of conduct in a realm that is generally characterised more by division and dispute than by consensus. The sceptic might protest that international norms are nothing more than wishful thinking. After all, our sceptic might observe, even the most prominent ostensible examples of international norms, such as the prohibition against intentionally targeting non-combatants in war, are regularly transgressed or evaded. Moreover, he or she might add, it would be difficult to argue that there is unanimous agreement on the source of authority for such principles. The sceptic might conclude that international moral norms are not even conceivable. In response, Mervyn Frost's careful account of what he calls 'settled norms' in international politics is extremely useful.

Frost has been a pioneering figure in normative IR theory. In a book first published in 1986, he defines 'settled norms' in international politics not as principles that are universally observed, or even uniformly grounded, but, rather, as principles for which there is a perceived need either to keep their infringement clandestine, or to provide special justification for any attempt to override or deny them.[13] In short, such principles are not openly transgressed without pointed justifications and excuses. They are tacitly respected, even in their breach. According to this understanding, 'settled norms' in international politics profoundly affect agents' behaviour, and specifically how they variously describe and defend, justify and judge, carry out and sometimes conceal acts and omissions.

12 As we will elaborate on below, by 'inform the behaviour' of an agent, we do not mean that a norm necessarily engenders compliance. Rather, a norm might inform the behaviour of an agent, and thus be discernible, by prompting attempts to justify, excuse, or hide its violation.

13 The first edition of Frost's book is *Towards a Normative Theory of International Relations* (Cambridge: Cambridge University Press, 1986). Page references in this chapter will be to the second edition: Frost, *Ethics in International Relations: A Constitutive Theory* (Cambridge: Cambridge University Press, 1996), 105-106.

Despite Frost's label of 'settled' norms, it is important to emphasise that international norms are not static. This point is highlighted in an important contribution to the mainstream constructivist literature on norms. In an influential article published in 1997, Martha Finnemore and Kathryn Sikkink propose that norms have a three-stage life-cycle: norm emergence; norm cascade (or broad norm acceptance) and internalisation.[14] In addition to usefully demonstrating the dynamic nature of international norms, their depiction of a process of normative change also reinforces both defining features of norms outlined above: their prescriptive and evaluative force,[15] and their broad acceptance and internalisation by the members of a specific community.[16] However, there are a few points that we suggest warrant attention before attempts are made to apply this concept without qualification to norms in cyberspace.

First, the focus of this particular article by Finnemore and Sikkink is on norms that are deliberately established by what they call 'norm entrepreneurs'. In one sense, this is especially relevant to the exploration of norms in cyberspace, where there has been a tendency (as noted above) to talk about cultivating, promoting and developing norms. However, we understand norms also to be the result of organic processes of emergence and change alongside conscious, concerted efforts to institutionalise them in particular forms. Indeed, one of our aims in this chapter is to highlight the need to acknowledge the significance and the consequences of the former before embarking on the latter. Second, the lifecycle of a norm, as presented by Finnemore and Sikkink, is something that strikes us as only possible to map with any accuracy retrospectively, which is not something that can yet be done in relation to expectations of right and wrong conduct in the context of the relatively new practices that currently define cyberspace. Our focus later in this chapter will be on identifying norms that at least begin to display features of what Frost has called a 'settled [international] norm' without analysing what stage they might be in a lifecycle that, we suggest, is still on-going in relation to Finnemore and Sikkink's proposed stages. Finally, there is a sense that the image of the lifecycle – through which expectations and codes of conduct evolve and gain progressively wider acceptance – does not allow for the regression or erosion of norms once they are established or widely accepted. We want to highlight that the dynamic process of normative change in cyberspace (like in any other realm) need not be, and is unlikely to be, linear according to some preconceived notion of an ideal endpoint.

14 Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organisation* 52:4 (1998), 887-1061 (895-905).

15 Finnemore and Sikkink emphasise that 'it is precisely the prescriptive (or evaluative) quality of 'oughtness' that sets norms apart from other kinds of rules'. Ibid, 891.

16 Note, however, that our conception of 'internalisation' differs from that of Finnemore and Sikkink in an important respect. They maintain that 'internalisation' entails 'a 'taken-for-granted' quality that makes conformance with the norm almost automatic'. Ibid, 904. For us, following Frost, what is taken for granted is the perceived need to justify, rationalise, excuse, deny or hide deviation from norm. Conformance need not be 'automatic' for a norm to be internalised. Its prescriptive and evaluative force is what is internalised.

2. A Fundamental Task: Interpreting Norms

A norm, we have argued, qualifies as such if it both displays prescriptive and evaluative force and is widely accepted and internalised by the members of a particular community. Cyberspace is a realm of principles, customs and codes of conduct that meet these two key criteria to various degrees. *Interpreting* these existing norms is the first crucial step before attempting to revise them, or to cultivate new norms. We need to explain what we mean when we claim the norms are things to be interpreted.

Interpretation is a process that we understand in terms of reading and deciphering the values, standards, and codes of conduct within a community in relation to a particular practice.[17] Importantly, this conception does not reduce norms to mere reflections of the *status quo*. Indeed, norms represent a rough consensus at a particular point in time on what *should* be done in a particular context. As such, norms are variously invoked to prescribe actions, tacitly acknowledged by agents in attempts to justify their infringement (as we learned from Frost), and appealed to in the censure of perceived violations. All of this means that interpreting norms demands more than a superficial reading of what is actually *done*. In other words, the objects of interpretation are not merely espoused principles or prevailing policies. Rather, they include the underlying values and shared understandings of the community in question, in relation to a particular practice, as revealed through agents' accounts of their own actions and the actions of others.

Frost's cogent definition of a 'settled norm', relayed above, helps to explain how international norms can be interpreted and studied. What is crucial in identifying a norm, according to Frost, is the perceived need to justify, excuse, rationalise, hide or deny any deviation from it. Any study of norms seeks to uncover our collective understandings of standards of right and wrong conduct. These are not revealed straightforwardly in what we do or refrain from doing, but rather in how we justify and judge acts and omissions. On this fundamental point, we might also turn to Michael Walzer's seminal 1977 book, *Just and Unjust Wars* – another key influence on normative IR theory. In this work, Walzer examines norms in the conduct of war, which he relabels 'the war convention'.[18] He argues that, in discerning these norms:

> '[i]t is important to stress that it is our judgments that are at issue here, not conduct itself. We cannot get at the substance of the convention by studying combat behaviour, any more than we can understand the norms of friendship by studying the way friends actually treat one another. The norms are apparent, instead, in the expectations friends have, the complaints they make, the

17 Our understanding of interpretation owes much to Michael Walzer's account in *Interpretation and Social Criticism* (Cambridge, Massachusetts: Harvard University Press, 1987).

18 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 125-222. Like our understanding of interpretation more generally, our reading of *Just and Unjust Wars* is influenced by Walzer's later book *Interpretation and Social Criticism*.

hypocrisies they adopt. So it is with war: relations between combatants have a normative structure in what they say (and what the rest of us say) rather than in what they do – though, no doubt what they do, as with friends, is affected by what they say.' [19]

Although working in a very different scholarly tradition, Finnemore and Sikkink make a similar assumption of how norms can be identified. They explain that 'because norms by definition embody a quality of 'oughtness' and shared moral assessment, norms prompt justifications for action and leave an extensive trail of communication among actors that we can study'. The illustration that they offer in support of this statement is useful, and reveals a means of deciphering norms similar to that proposed, respectively, by Walzer and Frost: '[f]or example, the US' explanations about why it feels compelled to continue using land mines in South Korea reveal that it recognizes the emerging norm against the use of such mines'. They conclude that '[i]f not for the norm, there would be no need to mention, explain, or justify the use of mines in Korea at all'.[20] As Walzer, Frost, Finnemore and Sikkink emphasise, in deciphering norms, it is necessary to pay attention to what agents say about their own and others' deviations from them.

Interpreting norms requires recognition of the broader systems of meaning and value within which they are situated, negotiated, and debated. Significantly, this means that even espoused principles and prevailing policies within a given community can be (internally) evaluated and criticised in relation to the community's norms, which must be carefully extracted from a complex context of contestation.[21] It also explains why, when interpreting norms, an appeal to a single source of espoused principles or even their codification in law is not enough. In relation to norms in the conduct of war, for example, Walzer emphasises the variety of sources that must be appealed to in the process of interpretation: 'we look to lawyers for general formulas, but to historical cases and actual debates for those particular judgments that both reflect the war convention and constitute its vital force'. He goes on to clarify that 'I don't mean to suggest that our judgements, even over time, have an unambiguous collective form. Nor, however, are they idiosyncratic and private in character'. Rather, '[t]hey are socially patterned, and the patterning is religious, cultural, and political, as well as legal'.[22] Tannenwald, writing almost thirty years later in the mainstream constructivist tradition (and citing the influence of

19 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 44.

20 Finnemore and Sikkink, 'International Norm Dynamics,' 892.

21 For accounts of an interpretive approach thus understood, which we associate with a critical stream of communitarianism, see the following: Walzer, *Interpretation and Social Criticism*; Walzer, *Spheres of Justice: A Defense of Pluralism and Equality* (New York: Basic Books, 1983); Walzer, '"Spheres of Justice": An Exchange,' *New York Review of Books* 30 (1983): 43-46; and Erskine, 'Whose Progress, Which Morals?' 463-464. According to such an approach, it is possible to challenge espoused principles and prevailing policies within a particular community by exposing their inconsistencies and tension with underlying values and social meanings. Walzer, for example, talks about the process of distinguishing 'deep and inclusive accounts of our social life from shallow and partisan accounts' in '"Spheres of Justice": An Exchange,' 43. For an assessment of the advantages and shortcomings of this critical communitarianism, see Toni Erskine, 'Qualifying Cosmopolitanism? Solidarity, Criticism, and Michael Walzer's 'View from the Cave,' *International Politics* 44 (2007): 135-36.

22 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations,* 45.

Walzer's approach in *Just and Unjust Wars),* describes norms not as 'governmental constructs' but rather as 'fundamentally cultural, religious and political phenomena' that, over time, 'emerge through a process of contestation and legitimation'.[23] Borrowing the words of James Turner Johnson, another central figure in normative IR theory in relation to work on the just war tradition, Tannenwald observes that 'in a given historical context, a great deal of work may be needed to define the content of a value that has begun to be seen dimly.'[24]

3. Three Challenges of the Cyber Domain

This task of interpreting norms is demanding in any domain, but there are reasons why it is particularly challenging, at this point in history, in the context of cyberspace. Namely, cyberspace is a realm of new practices, contested values, and often ambiguous agents. While we believe that these characteristics of cyberspace are well understood, their implications for addressing norms in this domain are not. In what follows, we will focus on these characteristics of cyberspace in relation to how they render the interpretation of norms – and, by extension, their promotion and revision – particularly difficult.

3.1 New Practices

Especially challenging contexts within which to interpret international norms are practices that are new, as yet not well understood, and quickly changing, such as those in the cyber domain. The rapidly advancing technology that defines cyberspace means that its constitutive practices are necessarily in flux. Referring specifically to the US military, Deputy Secretary of Defense William Lynn pointed out in 2010 that 'in less than a generation, information technology in the military has evolved from a tool for enhancing office productivity to a national strategic asset in its own right'.[25] Norms, as we have described them in the sections above, are necessarily the result of argument and negotiation within a community in relation to particular practices. They take time to evolve. As Walzer observed in relation to norms in the conduct of war, '[t]he war convention as we know it today has been expounded, debated, criticised, and revised over a period of many centuries'.[26]

New practices that have been emerging alongside the rapid development of cyberspace include those related to, for example, governing the global domain name system,

23 Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945,* 58.

24 Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945,* 58. For the original articulation, see James Turner Johnson, *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry* (Princeton: Princeton University Press, 1981), 167.

25 William J. Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy,' *Foreign Affairs* 89 (2010).

26 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations,* 45.

negotiating what is considered allowable content, individual network management, social media communication, coordination of on-line financial transaction protocols, and the anticipation of, protection against, and response to cyber attacks. It would be unreasonable to assume that the host of nascent and quickly changing transnational practices that are emerging in these areas have each already produced clear expectations regarding right and wrong conduct that are widely shared amongst, and inform the behaviour of, their participants. As we will demonstrate below, there *are* some principles that have begun to display the qualifying characteristics of norms in cyberspace. Nevertheless, the novelty and the relative instability of practices in cyberspace mean that there are likely to be fewer settled norms than in more established practices. It also, separately, renders more difficult the task of identifying those norms that have begun to emerge. Admiral Rogers' astute response to the charge of an apparent lack of progress in establishing norms in cyberspace is worth repeating. In the context of the discussion cited above, and drawing a comparison with what he described as the now-established norms relating to nuclear weapons, he noted simply that *'all of this has taken time,* and cyber is no different'.[27]

3.2 Competing Value Systems

A second complicating factor in attempting to identify norms in cyberspace arises not from the novel and dynamic nature of the evolving practices themselves, but rather from the tensions and even blatant contradictions between the various value systems that these globalised practices bring together. For example, competing understandings of the relationship between privacy, transparency and anonymity generate tension around differing perceptions of 'security' in cyberspace. For many western states premised upon notions of individual rights, anonymity is fundamentally linked to privacy and, from a civil liberties perspective, is therefore regarded as essential for a sense of personal security.[28] Although anonymity can be problematic for national security and law enforcement, these states are faced with the difficult task of trying to balance the necessity of identifying some individuals online with the protection of personal privacy, a task that requires some transparency of government and law enforcement practices. In states like China that adhere to more collectivist principles, anonymity can be seen to lead to a lack of accountability, which can be understood as a *threat* to the inextricably bound notions of personal and collective security.[29] Anonymity in this context is regarded as facilitating anti-social

27 Rogers, 'A Conversation with Mike Rogers.'

28 As President of Brazil, Dilma Rousseff pointed out, 'In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective 'democracy'. 'Speech by H. E. Dilma Rousseff, President of the Federative Republic of Brazil, at the Opening of the General Debate of the 68th Session of the United Nations General Assembly' (United Nations, The 68th Session of the United Nations General Assembly, New York 24 September 2013), http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

29 Although some sectors of Chinese civil society reject government control over Internet content and activity, others express a sense of concern about the implications of Internet technology for social cohesion. A recent Pew poll found that 75% of people polled in China regard the Internet as having a negative effect on morality, 62% feel it has a negative effect on politics and 57% feel it has a negative effect on personal relationships. Pew Research Center, *Internet Seen as Positive Influence on Education but Negative on Morality in Emerging and Developing Nations* (March 19, 2015), http://www.pewglobal.org/2015/03/19/3-influence-of-internet-in-emerging-and-developing-nations/.

behaviour such as trolling, and it is seen to undermine the transparency necessary for harmonious social interaction. Even if we can clearly identify and fully comprehend a particular cyber practice, the norms that begin to emerge in relation to it will necessarily be contested when the *underlying values* to which its participants appeal are radically different and sometimes incompatible.[30]

Yet another feature of this landscape of competing values is the diversity of actors and interests involved in cyberspace's emerging practices. It is important, for example, to remain alert to the significant role that the private sector plays in governing, developing and moderating Internet access, services and infrastructure. These actors are engaged in a delicate balancing act of trying to adhere to state demands and laws while also catering to the demands of their customers. The expectations of the two are not always in concert. Significantly, the underlying values of the private sector are oriented around the need to maximise profits. Inevitably, this shapes the practices that this sector engages in, and the interests that it brings to various negotiations about expectations and codes of conduct within them.[31]

Such clashes of values are deeply consequential when we are talking about norms. This is because, as we have argued, norms are necessarily embedded within broader systems of meaning and value. Interpreting norms in cyberspace requires that we pay attention to the types of competing values that we have just outlined. Importantly, currently conflicting values may change and even become more compatible over time as a result of prolonged interaction (between participants in particular transnational practices, for example), persuasion, negotiation, converging interests, the desire for reciprocity, shared goals or threats, and the perceived benefits of cooperation. Yet, an eventual convergence of values cannot be assumed. Practices in cyberspace whose participants are influenced by markedly different value systems may also experience the emergence of *competing* norms. Understanding norms in cyberspace demands attention to the complexities of their underlying values, as does any attempt to promote new norms or revise existing ones.

3.3 Ambiguous Agency

If we think of norms as widely-accepted expectations regarding conduct, then we also must consider to whom, or to what, these expectations can attach. Norms embody guidelines regarding what purposive actors should do and refrain from doing in certain contexts. In other words, these norms set out responsibilities which, to be met, must be attached to agents capable of understanding and discharging them. If norms in cyberspace outline expectations as to what is permissible, prohibited and required, to which agents do they apply? If one is to speak meaningfully about norms in cyberspace, it is necessary to identify the relevant *moral agents,* or bearers of duties, that are expected to adhere to the injunctions, imperatives and

30 Madeline Carr, *US Power and the Internet in International Relations: The Irony of the Information Age,* (London: Palgrave Macmillan, 2016); Madeline Carr, 'Public Private Partnerships in National Cyber Security Strategies', *International Affairs* 92 (2016), 43-62.

31 Madeline Carr, 'Public Private Partnerships in National Cyber Security Strategies.'

codes of conduct that we might variously interpret, negotiate, seek to shape, and strive to codify.[32]

Our starting-point here is that, alongside individual human beings, formal organisations such as states, non-governmental organisations (NGOs), multinational corporations (MNCs) and intergovernmental organisations are moral agents in world politics and crucial, and powerful, bearers of responsibilities in the cyber domain.[33] Yet, while the importance of identifying agents to which norms in cyberspace can be attached seems fairly straightforward, the often ambiguous nature of agency in cyberspace makes realising this endeavour difficult. This ambiguous agency is, in some instances, an inevitable result of what are, as yet, nascent practices. In others, it is a consciously-created feature of cyberspace resulting from values of privacy and anonymity.

Within the relatively new practices of cyberspace, the roles and responsibilities of particular agents are often ill-defined and poorly understood.[34] Moreover, and separately, this is a space of both human and non-human actors and, consequently, understanding 'machine-to-machine' agency in the context of the expanding 'Internet of Things' will be increasingly important to discussions of norms, specifically with respect to questions of attribution and perceptions of responsibility. Can semi-autonomous, and perhaps even autonomous, decision-making on the part of computers, for example, create the impression of mitigating responsibility on the part of more traditional purposive agents in world politics? The possibility that such 'machines' might be moral agents (or qualify as such in the future as their decision-making capacities become more sophisticated), and, separately, the *perception* that they carry this status, even in some attenuated form, both have far-reaching implications for how we understand assigning duties and apportioning blame in cyberspace. Although attempting to solve these specific puzzles is beyond the scope of this chapter, it is important to note that they contribute to the challenge of ambiguous agency in cyberspace and deserve further attention.[35]

With regard to the separate consideration of consciously-created ambiguous agency in cyberspace, individuals, states, and non-state actors can, in many cases, take actions with some expectation of anonymity. The challenges of attribution leave open opportunities for 'plausible deniability'. Actors responsible for illicit activities

32 To clarify, the label 'moral agent' does not describe good or somehow commendable actors (although they might, of course, be both); rather, it refers to those actors of whom we can reasonably have certain expectations. In very general terms, moral agents have capacities for deliberating over possible courses of action and their consequences and acting on the basis of this deliberation. These capacities render them vulnerable to the ascription of duties and the apportioning of moral praise and blame in the context of specific actions or omissions. See Toni Erskine, 'Making Sense of "Responsibility" in International Relations – Key Questions and Concepts,' in *Can Institutions Have Responsibilities? Collective Moral Agency and International Relations,* ed. Toni Erskine (New York: Palgrave Macmillan, 2003), 6-7.

33 See Toni Erskine, 'Assigning Responsibilities to Institutional Moral Agents: The Case of States and Quasi-States,' *Ethics & International Affairs* 15 (2001): 67-85 and 'Locating Responsibility: The Problem of Moral Agency in International Relations,' in *The Oxford Handbook of International Relations,* eds. Reus-Smit and Snidal.

34 A recent article by Mark Raymond and Laura DeNardis illustrates how the complex array of actors and practices involved in Internet governance is not well understood. Mark Raymond and Laura DeNardis, 'Multistakeholderism: Anatomy of an Inchoate Global Institution,' *International Theory* 7 (2015): 1-45.

35 See Erskine, 'Moral Responsibility, Artificial Agency and Dehumanized War' (Paper presented at the Oceanic Conference on International Studies, Melbourne, Victoria, 1 July 2014).

in cyberspace may maintain a posture of denial either when they believe they have successfully masked their identity or when they realise that for a prosecuting actor to present compelling evidence it would be necessary to reveal more about its own forensic capabilities than would be prudent. The motivations behind cyber attacks can be difficult to discern and state responses to belligerent behaviour (crime, terrorism or state use of force) fundamentally rely upon the identity and motivation of the perpetrator. Although many cyber attacks are blamed on governments, and despite many media and technical reports that suggest conclusive evidence, it actually remains unclear (at least, in the public domain) who was behind incidents like the 2014 Sony Pictures hack which prompted President Obama to impose further sanctions on North Korea as a form of retribution.

Given that identifying the relevant agents in the cyber domain that can discharge espoused responsibilities is fundamental to speaking coherently about how particular norms can be realised, both the fact that a clear understanding of relevant agents and their roles is often lacking in the context of particular practices and the capacity for actors to remain anonymous in cyberspace can be seen as significant impediments.[36] Nevertheless, in relation to the first problem, it is important to point out that defining responsibilities that accompany particular roles is part of the process of evolving norms within relatively new practices. With respect to the second concern of consciously-created ambiguous agency, responsibilities *can* be assigned (prospectively) and powerful expectations of right behaviour can be fostered in the context of cyber practices, even if the possibility of (retrospectively) apportioning blame and responding to delinquency is often made exceedingly difficult. Moreover, if we go back to Frost's account of 'settled norms' as principles for which there is a perceived need either to keep their infringement clandestine, or to provide special justification for any attempt to override or deny them, careful attempts to maintain anonymity and plausible deniability in cases of transgression can actually provide evidence of tacit acknowledgment of the norm itself.

36 Interestingly, if one adopts the definition of a norm cited frequently in mainstream constructivist work – namely, 'a standard of appropriate behaviour *for actors with a given identity*' – then the challenge of ambiguous agency would arguably impede the emergence of norms themselves and not just pose a challenge to how they are deciphered and applied in particular cases. This is the definition provided by Finnemore and Sikkink in 'Norm Dynamics and Political Change,' 891 (emphasis added), who, in turn, cite Peter J. Katzenstein's definition in 'Introduction: Alternatives Perspective on National Security,' in *The Culture of National Security: Norms and Identity in World Politics*, ed. by Peter J. Katzenstein, (New York: Columbia University Press, 1996), 5: 'The authors [in this volume] use the concept of *norm* to describe collective expectations for the proper behaviour of actors with a given identity'. However, our definition of a norm (influenced by work in political philosophy and normative IR theory and, we maintain, compatible with key assumptions underlying mainstream constructivist definitions), does not include this qualification. Indeed, we are not convinced this is a defining feature of all norms. After all, many norms, such as those associated with the conduct of war, are *general* prohibitions or prescriptions which relate to a particular practice rather than being tied to the identities of specific agents. Of course, some norms do define what we would call 'role responsibilities' or 'obligations'. (For an excellent account of this concept, see Michael O. Hardimon, 'Role Obligations,' *Journal of Philosophy* 91 (1994): 333–363). Such role-defining norms are important, but they do not exhaust the category of norm.

4. The Temptation of 'Quasi-Norms'

Attempts to address norms in the challenging context of cyberspace often fall into the trap of espousing *quasi-norms*. 'Quasi-norm' is a term that we have coined for the purpose of this chapter to refer to principles and codes of conduct that have been labelled 'norms', but that lack the key qualifying features of norms that we have identified above: namely, prescriptive and evaluative force, and wide acceptance and internalisation by the members of a particular community.[37] There are at least two common avenues along which those who espouse these merely purported norms seem to travel when it comes to discussions of cyberspace. The first is traversed by those who seek to 'create', 'implement' or 'impose' norms in this realm; the second by those who see their task as importing settled norms from distinct, but arguably comparable, realms.

4.1 'Quasi-Norms' as Normative Aspirations

It is not at all surprising to think that agents with particular interests or values will seek to impose rules and codes of conduct on practices that further these interests or values. This is a common, and often laudable, occurrence in discussions of cyberspace. Our very simple point is that these preferred principles and proposed rules *are not norms.* They are normative aspirations. Norms by definition are widely accepted and internalised by the members of a particular community. As such, they cannot be simply implemented or imposed. Rules might be imposed, norms cannot be. This is more than a mere semantic objection. The assumption that norms are things that can be imposed misses the crucial point that their power lies in the way they inform behaviour because agents have internalised their prescriptive and evaluative force. This conflation of norms with what are merely proposed rules and normative aspirations also overlooks potentially valuable strategies that might be adopted in fostering or cultivating norms, a point that we will return to in the conclusion.

4.2 'Quasi-Norms' as Imported Rules and Principles

Another context in which quasi-norms frequently appear in discussions of cyberspace is when attempts are made to import settled norms *from other realms* (in other words, norms that have evolved in the context of distinct practices) based on comparisons of the two realms. Our position here is that the comparisons themselves are understandable, and sometimes valuable, but that norms are not things that can logically be imported in this way.

It is often the case that analogies are drawn between relatively new and unfamiliar practices in cyberspace and those practices with which we are more acquainted. Indeed, a common, and frequently useful way to conceptualise a new phenomenon is through metaphor, invoking something that is already known in

37 We discovered subsequently that this is also a term used to describe a completely different phenomenon in algebra. Our focus, of course, is on ostensible 'norms' in international relations that do not, in fact, possess what we have argued are their defining characteristics.

order to come to grips with novelty. There are many examples of this strategy in relation to how cyberspace is represented and analysed. In the late 1980s, metaphors of transport infrastructure were common (the 'information superhighway', 'online traffic'). Metaphors from the health sector still shape the way we talk about cyber security ('viruses', 'infections', 'computer hygiene'). And, of course, some look for ways that language generally used to describe kinetic conflict can be invoked to help explain the daunting new reality of global cyber insecurity ('cyber war',[38] 'cyber deterrence',[39] 'cyber arms race'[40]). Yet, there is a danger to this strategy if we extend it to the attempt to uncover norms for cyberspace.

Practices in cyberspace do not simply map onto the very different practices from which these often-useful metaphors are drawn. This might seem a fairly straightforward point, yet the temptation to equate cyber practices with practices in other realms in the attempt to appropriate already-established, well-understood and influential standards of right and wrong conduct is strong enough to make it worth emphasising. For example, in some cases in which tropes and images from conventional warfare are borrowed in the attempt to make sense of cyber as an offensive tool, the logical next step is seen to be to appropriate the established (and often institutionalised) principles and codes of conduct from this purportedly analogous realm and transfer them to the cyber domain. A prominent example of this can be found in proposals to take principles from the just war tradition – principles which have evolved over centuries, if not millennia, in the context of practices that are very different to those of the cyber domain – and apply them to so-called cyber warfare.[41]

Attempts to relate a particular cyber practice under scrutiny to another, ostensibly similar, practice for which norms are already 'settled' are potentially valuable in terms of employing metaphors as heuristic tools to illustrate and interrogate specific features of the practice – and necessarily risky if the practices are conflated in the hope of thereby 'discovering' cyber-norms. If norms in international relations are understood to emerge, evolve, and be interpreted in the context of particular practices, they cannot be imported from one practice to another without risking significant loss of meaning and moral force.[42]

38 Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010); John Arquilla and David F. Rondfeldt, eds., *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica, CA: RAND Corporation, 2001). Thomas Rid critiques the term in *Cyber War Will Not Take Place*, 1st edn (Oxford University Press, 2013).

39 Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence* (Washington D.C.: National Defense University Press, 1996). Also Jason Ma, 'Information Operations to Play a Major Role in Deterrence Posture,' *Inside Missile Defense*, December 10, 2003.

40 Quote from US Cyber Command Director of Intelligence Samuel Cox, 'From our perspective, what we're looking at is a global cyber arms race [that] is not proceeding as a leisurely or even linear fashion but is, in fact, accelerating.' Cheryl Pellerin, 'DOD Expands International Cyber Cooperation, Official Says,' *American Forces Press Service*, April 10, 2012, http://archive.defense.gov/news/newsarticle.aspx?id=67889.

41 For such proposals to import just war norms and apply them to cyberspace, see, for example: Mariarosaria Taddeo, 'An Analysis For A Just Cyber Warfare,' in *2012 4th International Conference on Cyber Conflict,* ed. Christian Czosseck, et al. (Tallinn: NATO CCD COE Publications, 2012) and Luciano Floridi and Mariarosaria Taddeo, eds., *The Ethics of Information Warfare* (Switzerland: Springer, 2014).

42 Our criticism of attempts to 'import' norms from one practice to another – and thereby uproot them from the value systems in which they are embedded and the context in which they have been negotiated over time – is not directed at the process of 'grafting' that some mainstream constructivists, such as Richard Price, describe as a potentially effective means of norm promotion. See Richard Price, 'Reversing the Gun Sights: Transnational Civil Society Targets Land Mines,' *International Organization,* 52 (1998): 627-631. Understood as *part of the process of persuasion* undertaken by so-called norm entrepreneurs (which is how Price presents it), rather than as an attempt to simply implement or impose norms based on their acceptance in other realms, 'grafting' need not lead to quasi-norms.

In sum, unlike what we have labelled 'quasi-norms', norms evolve over time through necessarily complex and messy processes of contestation and negotiation in the context of the practices to which they are understood to apply. They can neither be imposed on a particular practice nor imported from one to another – although both moves might become tempting in the face of the obstacles outlined in the previous section and an accompanying impatience with the current stage of norm development in cyberspace. Nevertheless, despite the obstacles to both their emergence and interpretation, and what we have identified as the trap of appealing to 'quasi-norms', it *is* possible to uncover principles that have begun to qualify as norms. This can be done through the process of interpretation set out above.

5. Beyond Quasi-Norms in Cyberspace: The Norm of De-Territorialised Data

There are a number of frequently propounded principles and emerging codes of conduct in cyberspace that have at least begun to display the defining features of norms as we have identified them in this chapter. These include respective prohibitions against attacking critical infrastructure and against exerting sovereign control over digital information. The challenges that we articulated in section 3 render the process of these principles being established as norms extremely complex and multifaceted, and, relatedly, the task of attempting to interpret them as such particularly demanding. These principles are, after all, each articulated in relation to a new and rapidly-changing practice, each embedded in a system of values that is necessarily in flux and encounters challenges, and each associated with a fluid and often difficult-to-define constituency of agents. Determining whether each is a 'quasi-norm', proposed by particular agents, but lacking the defining features of norms, or, alternatively, has begun to display these defining features, is an important and daunting undertaking. We have suggested that such a problem might be addressed through a careful process of analysing explanations and evaluations of the principle's contravention by a broad cross-section of the agents who participate in the relevant practices. Although a comprehensive study of either one of these two principles would take us well beyond the scope of this chapter, in this section we will highlight examples of the types of judgements and justifications that would contribute to identifying a norm in such a study. Specifically, we will focus on the second of the two principles: namely, the prohibition against exerting sovereign control over digital information.

5.1 Underlying Values, Organic Processes of Evolving 'Shared Understandings', and 'Norm Entrepreneurs'

The expectation that data should be 'de-territorialised' emerged quite early in the development of Internet technology. It came about as a consequence of both conscious promotion by what Finnemore and Sikkink call 'norm entrepreneurs' (in this case, the US government) and the unintended, organic process (which we highlighted in section 1) of customs, mores and shared understandings being established over time between participants in a common practice. During the formative years of the development of Internet technology, an ideal of the world as open and connected through trade and the promotion of democracy and human rights was articulated by the Clinton-Gore administration. They framed these ideas as not only 'America's core values' but values with universal appeal.[43] Indeed, in a 1994 speech to the UN, US Vice President Al Gore described the Internet as 'a metaphor for democracy itself',[44] and suggested that '… as members of the same … vast, increasingly interconnected human family … we will derive robust and sustainable economic progress, strong democracies, … and, ultimately, a greater sense of shared stewardship of our small planet'.[45] In short, the free movement of data was explicitly associated with a proposed cosmopolitan ethos.

This approach was premised on an understanding of the universal nature of specific values including freedom of speech and freedom to access information. Importantly, this resonated strongly with the values of the technical community that was at the forefront of developing Internet technology.[46] This community placed a high premium on inter-operability, consensus-based decision making, and freedom to innovate exemplified in John Perry Barlow's 1996 *Declaration of the Independence of Cyberspace*.[47] The values of openness, freedom of information and minimal regulation over information flows became embedded in a broad global approach to Internet technology that passionately rejected the imposition of sovereign control over digital information.

These values have been reflected in statements by prominent political leaders. Indeed, the view of the global benefits of 'de-territorialised' digital information is routinely reinforced, often through the use of quite striking images. In one of her landmark speeches about Internet Freedom, Hillary Clinton referred to the Internet as 'a new nervous system for our planet' which implied indivisibility, interdependence and a united purpose.[48] She also made reference to the geopolitics of the Cold

43 Anthony Lake, 'From Containment to Enlargement' (Speech before the Johns Hopkins University School of Advanced International Studies, Washington, D.C., 21 September 1993, https://www.mtholyoke.edu/acad/intrel/lakedoc.html); and Warren Christopher, 'Building Peace in the Middle East' (Speech at Columbia University, 20 September 1993).

44 He uses the term 'global information infrastructure' at this point. Albert Gore Jr., 'Information Superhighways' (Speech before the International Telecommunications Union, 21 March 1994), http://vlib.iue.it/history/internet/algorespeech.htm.

45 Ibid.

46 Madeline Carr, *US Power and the Internet in International Relations: The Irony of the Information Age*.

47 John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (Davos, Switzerland, 8 February 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

48 Hillary Rodham Clinton, U.S. Department of State, *Remarks on Internet Freedom* (Washington D.C., 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

War by suggesting that 'a new information curtain is descending across much of the world' and '[s]ome countries have erected electronic barriers that prevent their people from accessing portions of the world's networks'.[49] The perceived imperative to prevent sovereign control over digital information is also framed as a global struggle in which each actor, state or non-state, must play a part. Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, urged delegates at the 2014 United Nations Internet Governance Forum to 'deliver what is needed to keep the internet open, unfragmented, and reliable. The time is now to ensure it develops further as a global source of empowerment, innovation and creativity for all'.[50] Kroes evoked arguably universal values by suggesting that the Internet is not 'just a technology' but also 'the new frontier of freedom and a new tool to exercise this freedom'.[51]

Interestingly, similar positive affirmations have issued from China despite that state's preference for a sovereign conception of cyberspace. President Xi Jinping delivered the keynote address to the second World Internet Conference in December 2015. In his speech, he emphasised that 'the Internet is a common space for mankind, and all countries should jointly build a community of shared destiny in cyberspace'.[52] He also called for all states to 'jointly foster a peaceful, secure, open and cooperative cyberspace and build a multilateral, democratic and transparent global Internet governance system'. [53]

Of course, even a principle that meshes with existing, underlying values, is actively backed by 'norm entrepreneurs', and also appears to have evolved organically through shared understandings between participants in transnational practices need not constitute a norm. At the very least, it represents a quasi-norm, or a normative aspiration. More work is required to establish that it meets the criteria to qualify as a norm.

5.2 Evidence of a Norm? Justifications and Judgements of Its Violation

In what follows, we will draw on the insights that we have taken from IR regarding both the nature of norms and the process of interpreting them in order to present evidence of what we call *the norm of de-territorialised data*. According to this principle, data in cyberspace should not be differentiated according to sovereign borders, but should, rather, be presented as a universal experience regardless of geography. In providing a preliminary case for the existence of this norm, we will demonstrate that this principle meets the two defining criteria outlined above; namely, it is: 1) understood to have prescriptive and evaluative force; and

49 Ibid.
50 Neelie Kroes, 'Defending the Open Internet' (European Commission, Opening ceremony of the Internet Governance Forum, Istanbul, 2 September 2014), http://europa.eu/rapid/press-release_SPEECH-14-576_en.htm.
51 Neelie Kroes, 'Protecting a Free Media in Azerbaijan' (European Commission, Speech at the Internet Governance Forum, Baku, 7 November 2012), http://europa.eu/rapid/press-release_SPEECH-12-784_en.htm.
52 Xi Jinping, Keynote Speech (Opening Ceremony of Second World Internet Conference, Wuzhen, 16 December 2015). Summary in English on the Chinese Embassy of the UK website, http://www.chinese-embassy.org.uk/eng/zgyw/t1325603.htm.
53 Ibid.

2) widely accepted and internalised by the members of the community of state and non-state actors who participate in a range of practices related to the flow of digital information. Specifically, we will suggest that a perceived prohibition against exerting sovereign control over digital information is discernible in actors' justifications and judgements of practices such as controlling online content (censorship), limiting access to certain online services, and, increasingly, seeking to exercise sovereign control over the physical location of stored data and the physical infrastructure of the Internet.

In 2011, the response to the introduction of the *International Code of Conduct for Information Security* put forward to the UN by China, Russia, Tajikistan and Uzbekistan, revealed a strong perception that any violation of the principle that digital information is borderless demands a justification. The Code called for compliance in cyberspace with 'universally recognised norms [including] the sovereignty, territorial integrity and political independence of all states'.[54] This was necessary, the document suggested, in part as a consequence of the extent to which online data 'undermines other nations' political, economic and social stability, as well as their spiritual and cultural environment'. This was met with approbation in the US with Jason Healey referring to this passage specifically as 'standard boiler plate from autocratic countries to limit freedom of expression'.[55] Michele Markoff, the US State Department's Senior Policy Adviser on Cyber Affairs, also described the Code as an attempt by the proposing states to 'justify the establishment of sovereign government control over Internet resources and over freedom of expression in order to maintain the security of their state'.[56]

This perceived need to justify sovereign control is significant. With reference to Frost's work, we have argued that establishing the existence of a norm does not require demonstrating that a principle is universally adhered to. (Indeed, if this were the qualifying criterion, it would be impossible to defend the existence of *any* international norms.) Rather, a principle is tacitly acknowledged as a norm when there is a perceived imperative to justify or deny its violation. Or, as Richard Price, a mainstream constructivist scholar, argues following a similar logic, 'one can say that a norm exists when the dominant discourse shifts in such a way that puts opponents on the defensive'.[57]

China recently demonstrated this perceived need to account for deviating from the principle of de-territorialised data. In the same speech before the World Internet Conference in which he commended the concept of a global commons in

54 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://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

55 Jason Healey was the Director for Cyber Infrastructure Protection at the White House under President George W. Bush. At the time of these comments, he was Director of the Cyber Statecraft Initiative at the Atlantic Council. Jason Healey, 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms,' *The Atlantic Council Blog*, September 21, 2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/breakthrough-or-just-broken-china-and-russia-s-unga-proposal-on-cyber-norms.

56 Gerry Smith, 'State Department Official Accuses Russia and China of Seeking Greater Internet Control,' *Huffington Post*, September 28, 2011, http://www.huffingtonpost.com/2011/09/27/russia-china-internet-control_n_984223.html.

57 Price, 'Reversing the Gun Sights: Transnational Civil Society Targets Land Mines,' 631.

cyberspace, President Xi engaged with a different conception of freedom to that used by Neelie Kroes. He linked freedom to order by saying that 'order is the guarantee of freedom' and therefore, it is necessary to respect sovereign law in cyberspace 'as it will help protect the legitimate rights and interests of all internet users'.[58] In a similar effort to justify exercising domestic law (and thereby infringing the norm of de-territorialised data), US Senator Patrick Leahy made the following comments when introducing a bill designed to prevent 'foreign-owned and operated' websites from facilitating intellectual property theft: 'We cannot excuse the behaviour because it happens online and the owners operate overseas. The Internet needs to be free – not lawless'.[59] This tension between the desire to apply domestic law to digital information that does not remain tethered by geography and the promotion of an online experience that transcends territorial borders is a common framework within which justifications for imposing sovereign control are put forward. What is important here is not exactly *how* these actors account for their failure to adhere to the principle of de-territorialised data, but the perceived need to do so.

National security is increasingly provided as justification for imposing sovereign control on digital information. Again, the perceived imperative to justify this action is revealing. In November 2015, days after the terrorist attacks in Paris (and making explicit reference to them), UK Chancellor George Osborne defended the passage of the Investigatory Powers Bill (otherwise known in the UK as the 'Snoopers' Charter') by arguing that 'when the internet was first created, it was built on trust. That trust, appropriate inside a community of scholars, is not merited in a world with hostile powers, criminals and terrorists'. In other words, the prohibition against exerting sovereign control over data is tacitly acknowledged in the argument that it must be overridden due to what is presented as an extreme, dangerous security situation. (This is analogous to 'supreme emergency' arguments in Walzer's account of the war convention.)[60] Indeed, Osborne goes on to link the vulnerabilities of UK critical infrastructure with concerns that 'ISIL's murderous brutality has a strong digital element'. Consequently, he argues, '[o]nly government can defend against the most sophisticated threats, using its sovereign capability. And that's exactly what we will do'.[61] Extreme threats to security are invoked as rationales for violating the prohibition against sovereign control over digital information.

The Snowden revelations in 2013 have also been employed as justification by many states for bringing digital information more firmly under sovereign control.[62]

58 Xi, keynote speech at the Second World Internet Conference, 2015.

59 Patrick Leahy, 'Senate Judiciary Committee Advances Bipartisan Bill to Combat Copyright Infringement and Counterfeits,' November 18, 2010, http://www.leahy.senate.gov/press/senate-judiciary-committee-advances-bipartisan-bill-to-combat-copyright-infringement-and-counterfeits.

60 See the discussion of tacitly acknowledging norms through such 'supreme emergency' justifications of their violation in Erskine, *Embedded Cosmopolitanism*, 189, 194. For Walzer's original 'supreme emergency' argument, see Walzer, *Just and Unjust Wars,* 251-268.

61 George Osborne, 'Chancellor's Speech to GCHQ on Cyber Security' (Delivered at Government Communications Headquarters, Cheltenham, 17 November 2015), https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

62 Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders,' *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, May 1, 2014, http://ssrn.com/abstract=2430275.105.

In 2015, citing the potential for human rights abuses, the EU revoked the Safe Harbour Act which had allowed the personal data of EU citizens to be stored in the US.[63] The EU Commissioner responsible for data protection, Věra Jourová, pointed out that this was not simply a matter for the US, but that it applied to 'the conditions to transfer data to third countries, whatever they may be'.[64] This 're-territorialisation' of digital information has also been extended to the physical infrastructure across which data travels. Having previously called the Internet a 'CIA project' and following what he regarded as biased reporting in the western media of the conflict in Crimea, Russian President Vladimir Putin announced plans to develop the capacity to segregate Russian cyberspace in case of '*emergencies*'. The proposal would potentially bring the .ru domain under state control, which Russian newspapers reported would strengthen Russia's sovereignty in cyberspace.[65] Presidential aide and former Minister of Communications and Mass Media, Igor Shchegolev, explained that this had become necessary due to the unpredictability of western politicians and businesses.[66] He linked the Russian state's concerns to the Internet outage experienced by Syria in 2012, which some attribute to the US. Again, what is particularly noteworthy in these cases of statements by both the EU and Russian political leaders is the perceived imperative to explain any deviation from the principle of de-territorialised data.

This brief analysis does a number of important things. First, it demonstrates that the prohibition against exerting sovereign control over digital information at least begins to meet our two qualifying criteria of a norm. The norm of de-territorialised data is not without challenges, but both its prescriptive force and wide acceptance and internalisation amongst participants in transnational practices related to the digital flow of information are evident in the pervasive perceived need to justify its violation. Second, in providing evidence for this norm of de-territorialised data, this case illustrates how norms might be interpreted in cyberspace through detailed attention to the way that states and other agents variously justify and rationalise their own actions and judge the actions of others. The task of interpreting cyberspace's normative terrain cannot rely on superficial observations of agents' conduct. Third, this analysis reiterates significant features of our account of norms, inspired by prominent positions in IR: that norms are firmly embedded in broader systems of values; that both deliberate attempts to foster, shape and institutionalise principles in particular forms *and* organic, unplanned processes of negotiation and contestation in the context of evolving, shared practices contribute to the emergence of norms; and that norms, carefully interpreted, are distinct from, and can be invoked

63 This was initiated through a court case brought by Max Schrems who highlighted the flaws in the Safe Harbour Act with respect to Facebook. Europe v Facebook, http://europe-v-facebook.org/EN/en.html.

64 Věra Jourová, 'Commissioner Jourová's Remarks on Safe Harbour EU Court of Justice Judgement before the Committee on Civil Liberties, Justice and Home Affairs' (European Commission, Speech before the Committee on Civil Liberties, Justice and Home Affairs, Strasbourg, 26 October 2015), http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm.

65 Luke Harding, 'Putin Considers Plan to Unplug Russia from the Internet "in an emergency"', *The Guardian*, September 19, 2014, http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow.

66 '"Unpredictable West" Could Isolate Russian Internet, Putin's Aide Warns,' *RT*, October 17, 2014, https://www.rt.com/politics/196848-russia-internet-west-plan/.

to challenge, espoused principles and prevailing policies when these are at odds with a community's deeper commitments and tacitly acknowledged values.

6. Conclusion

Three quite different lessons can be drawn from our preliminary analysis, each of which points to areas of further study.

First, and at the level of *how* one might go about studying cyberspace's rapidly changing normative landscape, two areas of scholarship within the discipline of IR – normative IR theory and mainstream constructivism – have produced rich and diverse bodies of work on the nature of norms in international relations that together provide an invaluable starting-point. The combined insights of both approaches offer a nuanced conceptual understanding of norms and an account of how they might be deciphered in a challenging context such as cyberspace. Notably, these two approaches to norms have developed largely independently of each other (a curious and all-too-common occurrence when it comes to different 'camps' within the discipline of IR).[67] Further work on the points of commonality and divergence between normative IR theory and mainstream constructivist approaches to norms in international relations has the potential to refine and bolster the arguments of each – and to contribute to sophisticated analyses of emerging norms in cyberspace.

Second, and related to the ambitious attempts to 'cultivate' and 'promote' norms in cyberspace noted above, the chapter repeatedly gestures towards a crucial caveat. For norm promotion to be effective it is not only proposed principles or codes of conduct that must be the objects of such efforts. Rather, the broader systems of underlying values in which norms necessarily emerge and are embedded must also be the focus of analysis, and possibly persuasion, negotiation and concerted attempts at revision over time. Neglect of the complex context in which international norms must be situated leads to the promotion of quasi-norms, which may be clear statements of preferred principles on the part of certain actors, but lack the prescriptive force and collective acceptance that make norms so powerful in international relations. Attempts might be made to cultivate or revise norms, but the success of such endeavours depends on whether they are consistent with (and cognisant of) the broader systems of meaning and values already accepted – and always contested and open to re-negotiation – by the members of a particular community.

Third, the chapter suggests that interpreting existing norms in cyberspace – such as the proposed norm of de-territorialised data – might yield results that are,

67 For accounts of the costs of the discipline's division into competing theoretical and methodological 'camps' see David A. Lake, 'Why "Isms" Are Evil: Theory, Epistemology, and Academic Sects as Impediments to Understanding Progress', *International Studies Quarterly* 55 (2011): 465-80 and Erskine, 'Whose Progress? Which morals?', 449.

perhaps surprisingly, out of step with normative change in other realms of international relations. Our brief analysis above uncovers an established cosmopolitan norm in cyberspace that eschews sovereign jurisdiction and political borders. The study also suggests that this norm of de-territorialised data is facing a new emerging norm in cyberspace: one that we might call the *norm of sovereign control over data.* In other words, the norm of de-territorialised data is already in the process of being challenged, and perhaps eclipsed, by a competing norm.[68] Notably, this apparently emerging opposing norm is, in fact, one that seems to map closely onto the long-established norms in international relations of state sovereignty and territorial integrity – norms that have recently been challenged by the emerging cosmopolitan norm of humanitarian intervention in response to mass atrocity. In short, the normative change that we have begun to uncover in cyberspace seems to be the reverse of what has been occurring in the context of the recent endorsement and institutionalisation of the proposed 'responsibility to protect' and its accompanying claim of contingent sovereignty. These very different patterns of normative change warrant further attention – as does the fascinating case of competing norms regarding the jurisdiction of data in cyberspace.

International norms in cyberspace are the product of, *inter alia*, negotiation and contestation over time in the context of evolving transnational practices, accompanying shifts in dynamic, underlying value systems that variously conflict and overlap, political compromise between multiple national and private interests, pragmatic agreements, serendipitous convergences, attempts at carrot-and-stick persuasion by the most powerful actors, and the socialisation of these same powerful agents. In short, they are the product of both chance and design, cooperation and conflict, emerging collective identities and changing conceptions of self-interest. The important point that we have tried to highlight is that we need to understand where we currently are in terms of expectations, values and perceived constraints in cyberspace in order to navigate – and perhaps even attempt to shape or radically revise – the complex normative terrain. This, in turn, requires a sophisticated understanding of both the concept of norms and how they operate in cyberspace.

68 The changing constitution of the community within which norms regarding the jurisdiction of data have been negotiated seems relevant to us – and demands further attention. There was certainly a concerted effort by the US government to promote values of free movement of data, but there had also been a more organic process on the part of the (transnational) technical community, for whom these values had been firmly established and informed the early development of the Internet. The values of the technical community happened to synergise with US policy in the context of the norm of de-territorialised data and served to reinforce it. However, as this issue of data jurisdiction has shifted from the transnational technical community to state leaders in international political negotiations, arguably competing value systems have become more prominent.

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.

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

CHAPTER 7

Confidence-Building Measures in Cyberspace: Current Debates and Trends

Patryk Pawlak

1. Introduction

The rapidly shifting global digital environment is raising concerns about the sustainability of the positive contribution that the Internet has made towards economic and human development.[1] Since the end of the 1990s, when the debate about the impact of information and communication technologies on international security was first raised on the international agenda, the number of Internet users has grown over a thousand-fold from just 3 million in 1990 to over 3.2 billion in 2015 and is expected to reach 4.7 billion by 2025.[2] Most of this growth will continue to come from developing countries, including countries in Asia and Africa. The number of mobile devices is already higher than the world's population.[3] Digital environment and threat landscape are changing too: state and non-state actors increasingly exploit vulnerabilities in cyberspace to gain advantage over their competitors and adversaries.[4] The assessment of national cyber security programmes conducted by UNIDIR in 2012 has shown that an increasing number of states give some role to the armed forces.[5] Research also shows that out of 15 largest military spenders, 12

1 Patryk Pawlak, ed., European Union, Institute for Security Studies, *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development*, Report No. 21 (December 2014), http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf.

2 David Burt, et al, Microsoft, *Cyberspace 2025. Today's Decisions, Tomorrow's Terrain. Navigating the Future of Cybersecurity Policy* (June 2014).

3 CISCO, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014-2019: White Paper* (3 February 2015), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

4 Symantec, *The 2015 Internet Security Threat Report (ISTR20)*, vol. 20 (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

5 James Andrew Lewis and Götz Neuneck, *The Cyber Index: International Security Trends and Realities* (New York and Geneva: United Nations Institute for Disarmament Research, 2013), http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

are developing dedicated cyber warfare units and two-thirds appear to possess or be developing offensive cyber capabilities.[6]

As Internet-based platforms and infrastructure continue to grow in importance for the delivery of basic services and become part of critical national infrastructure, the risk of conflict resulting from misunderstandings or misperceptions between countries becomes more acute. To reduce the possibility of such a scenario materialising, the international community has engaged in several regional or global processes focused on clarifying how the existing international law applies to cyberspace, development of norms of responsible state behaviour, and development of confidence-building measures (CBMs). The overarching link for these efforts has been provided by four consecutive United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGEs). However, there is a growing concern that the concepts, methods and measures developed by various regional and international forums may evolve in diverging directions further contributing to uncertainty.

The aim of this chapter is to investigate the evolution of confidence-building measures in cyberspace, their features, main trends, and possible trajectories for development in the future. Even though building confidence in cyberspace is a process that requires the involvement of all layers of society – as demonstrated by a large breadth of contributions in this volume – this chapter investigates solely the evolution of confidence-building measures between states and state institutions at bilateral, regional or international level.[7] However, the chapter also notes the increasing focus on capacity-building in strengthening the implementation of CBMs. The chapter concludes with the presentation of two distinct models illustrating how norms, CBMs and capacity-building contribute to stability in cyberspace.

2. Uncertainty in Cyberspace

With cyber security attracting increasing interest and the barriers for access to cyber capabilities decreasing, the risk of a conflict resulting from misunderstandings and miscalculation is also growing. The reliance on ICT platforms for delivery of government, financial and public services makes their users vulnerable to cyber attacks by organised criminal groups or foreign governments.

Because cyberspace enables certain levels of anonymity, state, state-sponsored and non-state actors do not shy from exploiting these vulnerabilities. The first report of the UN GGE delivered in 2010 stressed that 'uncertainty regarding attribution and the absence of common understanding regarding acceptable state behaviour may create the

6 Ibid.
7 See chapters 10, 11 and Appendix 1 for private sector perspectives.

risk of instability and misperception.'[8] The difficulties with attribution of attacks give states the ability to deny responsibility,[9] as has been the case for the North Korean government which has consistently denied any involvement in the cyber attacks on Sony Pictures Entertainment.[10] The challenges related to attribution are even more daunting if one takes into account the possible consequences of an erroneous attribution and a relatively easy access to instruments for conducting cyber attacks by cyber criminals and hackers. For instance, the cyber attacks against TV5 Monde initially attributed to ISIL/Da'esh were later re-attributed to attackers based in Russia.[11] On the other hand, malware discovered on the Nasdaq servers in 2014 was initially assessed as originating from the Russian Federal Security Service and capable of destroying the content of the entire stock exchange; it was subsequently found to be less destructive and planted by two Russian hackers.[12]

The protection of cyberspace and reducing its vulnerability to digital threats has become a key element of national security strategies. While a substantial part of the adopted solutions are of non-military nature (legislation, organisational adaptation and training), many countries have been also investing in offensive and defensive cyber capabilities of military nature.[13] The risk is, however, that the progressing militarisation of cyberspace and the reliance on new systems of state-owned cyber weapons[14] similar to *Red October*, *Flame*, *Duqu* or *Stuxnet* will accelerate the cyber arms race, and competition for 'digital supremacy'[15] ultimately increasing the risk of escalation and conflict. Militarisation and expansion of cyber weapons is also problematic due to the ambiguity concerning qualification of a cyber attack as a use of force under Article 2(4) of the UN Charter, and the threshold for self-defence as stipulated in Article 51.[16] Establishing whether a cyber attack constitutes an armed attack, if the use of force is legitimate (*jus ad bellum*), and how force can be employed (*jus in bello*) is still a subject of a debate among international legal scholars and policymakers.[17]

8 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010), http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

9 Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38 (2014): 4-37, https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf.

10 David E. Sanger and Nicole Perlroth, 'U.S. Said to Find North Korea Ordered Cyber Attack on Sony,' *The New York Times*, December 17, 2014, http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0; 'NorthKorea Proposes Joint Sony Hack Inquiry with US,' *BBC News*, December 20, 2014, http://www.bbc.com/news/world-us-canada-30560712.

11 Adam Thomson, 'ISIS Hackers Cut Transmission of French Broadcaster,' *Financial Times*, April 9, 2015, http://www.ft.com/cms/s/0/5f419994-de94-11e4-8a01-00144feab7de.html#axzz3wSJjk22o; 'APT28: A Window into Russia's Cyber Espionage Operations?' *FireEye*, October 27, 2014, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

12 Benjamin Brake, *Strategic Risks of Ambiguity in Cyberspace*, *Contingency Planning Memorandum No. 24* (Council on Foreign Relations, 2015), http://www.cfr.org/cybersecurity/strategic-risks-ambiguity-cyberspace/p36541.

13 Lewis and Neuneck, *The Cyber Index: International Security Trends and Realities.*

14 Gary D. Brown and Andrew O. Metcalf, 'Easier Said than Done: Legal Reviews of Cyber Weapons,' *Journal of National Security Law and Policy* 7 (2014): 115-138, http://jnslp.com/wp-content/uploads/2014/02/Easier-Said-than-Done.pdf.

15 Kenneth Geers, et al, FireEye, *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks* (2014), https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf.

16 The UN General Assembly Resolution 3314 (XXIX) defines aggression as 'the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations.' UN General Assembly resolution 3314 (XXIX), *Definition of Aggression*, 3314 (XXIX) (14 December 1974), http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement. See also Michael N. Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context,' in *4th International Conference on Cyber Conflict: Proceedings*, eds. Christian Czosseck, Rain Ottis and Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2012).

17 See: Schmitt, '"Attack" as a Term of Art in International Law.'; Michael N. Schmitt, 'Classification of Cyber Conflict', *Journal of Conflict and Security Law* 17 (2012): 245-260, http://jcsl.oxfordjournals.org/content/17/2/245.full; Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

3. Confidence-Building Measures and Norms: Two Sides of the Same Coin

Confidence-building measures are one of the key mechanisms in the international community's toolbox aiming at preventing or reducing the risk of a conflict by eliminating the causes of mistrust, misunderstanding and miscalculation between states.[18] Most of the existing confidence-building measures date back to 1975 when the Helsinki Final Act[19] was adopted, followed by the 1986 Stockholm Document on Confidence- and Security-Building Measures and Disarmament in Europe,[20] and the 1990 Vienna Document.[21] Military confidence-building measures aim to prevent a potential outbreak of military conflict by improving relations between government officials and militaries.[22] Their primary focus is on increasing transparency, improving information exchanges, and restraining the use of violence by armed forces. The assumption is that exchange of information about military doctrines and resources contributes to stability by enhancing situational awareness and building common understandings. However, while CBMs can contribute to de-escalating an unintended conflict, they are of limited use when conflicts are fuelled intentionally.

The reports on the implementation of United Nations General Assembly Resolution 65/63 of 2011 concerning information on confidence-building measures in the field of conventional arms indicate three main categories of military CBMs: communication and information exchange measures; transparency and verification measures; and military restraint measures.[23] Non-military confidence-building measures are used to preserve peace by building trust between communities, including law enforcement, incident responders, or civil society, through actions or processes undertaken across political, economic, environmental, social or cultural fields.[24] Both have a number of objectives in common: to prevent armed conflict; limit violence; and ideally provide foundations for sustainable

18 Daniel Stauffacher, ed. and Camino Kavanagh, rap., ICT4Peace Foundation, *Confidence Building Measures and International Cyber Security: Cyber Policy Process Brief* (2013), http://ict4peace.org/wp-content/uploads/2015/04/processbrief_2013_cbm_wt-71.pdf.

19 'Conference on Security Co-operation in Europe: Final Act' (Organization for Security and Co-operation in Europe, Conference on Security Co-operation, Helsinki, 1975), https://www.osce.org/mc/39501?download=true.

20 'Document of the Stockholm Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation in Europe' (Organization for Security and Co-operation in Europe, 19 September 1986), https://www1.umn.edu/humanrts/peace/docs/stockholm1986.html.

21 'Vienna Document 1990 of the Negotiations on Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Vienna Meeting of the Conference on Security and Co-operation in Europe' (Organization for Security and Co-operation in Europe, Vienna, 17 November 1990).

22 United Nations, General Assembly, *Special Report of the Disarmament Commission to the General Assembly at Its Third Special Session Devoted to Disarmament*, A/S-15/3 (28 May 1988), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/S-15/3%28SUPP%29&Lang=E.

23 United Nations, General Assembly, *Information on Confidence-Building Measures in the Field of Conventional Arms: report of the Secretary-General*, A/66/176 (25 July 2011), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/429/12/PDF/N1142912.pdf?OpenElement.

24 'OSCE Guide on Non-Military Confidence-Building Measures (CBMs)' (Organization for Security and Co-operation in Europe, Vienna, 2012), http://www.osce.org/cpc/91082?download=true.

cooperation. However, developed in an entirely different context – namely to build confidence with regard to the proliferation and use of conventional weapons – the traditional approach to military and non-military CBMs requires certain adaptations in order to adequately reflect the specificity of the digital domain (Table 1).

The discussion about confidence-building measures in cyberspace is closely linked to the parallel debates about acceptable norms of state behaviour. While the focus on norms, both in the existing international law and non-binding political agreements, helps to establish international level of expectations about states' behaviour in cyberspace, development of CBMs provides practical tools to manage these expectations.[25] For instance, the norm according to which states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs creates an expectation that states will use all instruments at their disposal to prevent such unlawful acts from occurring. Hence, it creates a concrete expectation among states. However, such expectations need to be adjusted, taking into account the capacities of individual states to meet their obligations. Confidence-building measures facilitate such adjustments, for example through establishing channels of communication, information exchange and practical cooperation during investigations. The UN GGE 2015 report, for instance, stipulates that 'in case of ICT incidents, states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences'. Confidence-building measures focusing on transparency and communication provide the necessary foundation for operationalisation of this norm. Without confidence-building measures in place, even legally binding norms enshrined in international treaties only provide an illusion of stability and normalcy.

Differences in the interpretation of the UN GGE 2015 report despite an agreement on a concrete set of norms, also show that there is still certain level of uncertainty which, if not addressed, may contribute to escalation of a conflict.[26] For instance, the report contains a compromise on the use of Article 51 of the UN Charter which gives states the right to individual or collective self-defence in case of armed attacks.[27] However, according to the Russian special envoy for international cooperation in information security, Andrei Krutskikh, 'there is no general idea in the world today what is meant by the 'armed attack' in relation to the use of ICTs'.[28]

25 For a detailed analysis of legal aspects of CBMs, see Katharina Ziolkowski, *Confidence Building Measures for Cyberspace - Legal Implications* (Tallinn: NATO CCD COE Publications, 2013), https://ccdcoe.org/publications/CBMs.pdf.

26 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), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

27 The compromise language reached in the UNGGE does not make a specific reference to Article 52 of the UN Charter but to the Charter in its entirety. United Nations, General Assembly, *Group of Governmental Experts*, A/70/174.

28 'UN Cybersecurity Report Compromises on Self-Defence Issue – Russian Official,' *Sputnik International*, August 17, 2015, http://sputniknews.com/politics/20150817/1025819426/UN-cybersecurity-report-compromises-on-self-defence.html.

Table 1. Traditional CBMs and cyber-related adaptations.[29]

Aim of a measure	Examples	Suitability in cyberspace
Communication and information exchange measures		
Enhancing mutual understanding of national military capabilities and activities through facilitating regular communication	Military points of contact, hotline between chiefs of the armed forces, exchange of military information on national forces and armaments, advance notification of important military exercises	Feasible but require a clear definition of 'cyber military capabilities' and clear separation of military and civilian capabilities
Transparency and verification measures		
Monitoring of military facilities and activities, primarily in order to ensure that a party's military activities are of a non-aggressive nature	Inviting observers to monitor major military exercises, verification missions on-site	Difficult to implement given the dual-nature of cyber-tools and countries' interest in preserving strategic ambiguity concerning their capabilities
Military restraint measures		
Limiting the capacity of parties for (surprise) offensive military attacks	Restrictions on major military exercises, limitations of troop movements, demilitarised and weapon-free zones	Difficult given the civil-military nature of Internet and lack of transparency. Requires a definition of 'weapon-free zones' in cyberspace in terms of ICT infrastructure and not necessarily linked to geography
Political measures		
Strengthening the confidence in the political system	Power sharing arrangements, proportional recruitment for state and regional institutions, electoral reforms, or decentralisation of power	Feasible through non-discriminatory legislative frameworks, respect for norms, rule of law and human rights; clear division of competences and institutions in place; national cyber security strategy
Economic measures		
Reducing the risk of a conflict through increasing trade and economic interdependency	Trade agreements, customs areas	Feasible through export control mechanisms and increasing dependence on cyberspace for economic growth and development
Environmental measures		
Providing incentives for cooperation in the areas of crisis/disaster management or management of resources	Concrete cooperative measures addressing natural hazards: earthquakes, floods, fires	Feasible through concrete cooperative measures in case of cyber incidents, i.e. CERT-to-CERT
Societal and cultural measures		
Strengthening ties between communities or nations	People-to-people dialogues and joint projects (i.e. exchanges of students)	Feasible through ensuring open access to the Internet, in particular social media but also online services

29 Author's compilation based on Lewis and Neuneck, *The Cyber Index: International Security Trends and Realities.*

It is also important to understand that international law, even though legally binding and applicable to cyberspace, is not a silver bullet for solving the challenges linked to uncertainty in cyberspace. The UN GGE 2013 report reaffirmed that 'international law, and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'.[30] However, successive reports have acknowledged the need to better understand how this should be done in practice. CBMs contribute to this process by establishing certain foundations for the debate. They serve as tools for ensuring that states have the same understanding of the normative commitments that they made and are bound to respect. For instance, they may serve as socialisation venues through which actors exchange information about mutual expectations, practices, and working methods, which in turn influences the level of trust and the commitment to certain normative frameworks. Consequently, the processes of development of norms and CBMs are closely linked and interdependent. If norms serve as a certain ideal of behaviour that states aspire to, an adequate mix of CBMs – ranging from those improving situational awareness to building resilience and facilitating cooperation – is supposed to help states achieve them (see Table 2).

In addition, whereas CBMs can prevent unintentional conflicts by stopping or slowing down the spiral of escalation, their usefulness is limited in case of intentional conflict and escalation. Consequently, achieving the full potential of confidence-building measures to minimise misperceptions may be limited by a number of factors that undermine credibility of the parties involved: a limited political will and commitment to preventing a conflict, such as a threat to resort to offensive capabilities as opposed to law enforcement and other alternative approaches; distribution of resources by investment in defence rather than resilience and skills; a weak legal system, such as ineffective rule of law and administration of justice; or recurring hostilities such as cyber attacks.

4. How Do States Build Confidence in Cyberspace?

The foundations for the discussion about the confidence-building measures in cyberspace have been laid down by successive UN GGE reports and quickly became part of the effort undertaken within regional organisations in Europe, the Americas and Asia, albeit with a different focus and results.

4.1 United Nations

Even though United Nations does not work on developing specific CBMs, leaving this task to regional organisations, the initiatives undertaken at the UN level shape a common understanding of the role of CBMs within a larger debate about stability in

30 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.

cyberspace. The issue of information security in the international context was introduced to the United Nations agenda by Russia in 1998.[31] Since then, the Secretary-General to the General Assembly has presented annual reports laying out the views of Member States. In its submission to the 2003 report, Russia put forward the idea of establishing an international group of governmental experts which would analyse international legal provisions relating to various aspects of international information security and study existing concepts and approaches.[32] The group was convened for the first time in 2004[33] but was not able to reach consensus on the final report due to the 'complexity of the issues involved'.[34] The UN GGE 2010 report further highlighted the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to state use of ICTs, which could affect crisis management in the event of major incidents, and called for new measures, including to 'build confidence, reduce risk and enhance transparency and stability'.[35] The UN GGE 2013 report went further in stating that 'voluntary confidence-building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception'.[36]

The real breakthrough came with the most recent report of the Governmental Group of Experts established in 2014.[37] The UN GGE 2015 report recommends that, consistent with the purposes of the United Nations, states 'cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security'.[38] It reiterates some of the measures suggested in the earlier report but also pays particular attention to measures aimed at reducing the risks of misperceptions and conflicts linked to the attacks on ICT-enabled infrastructure (Table 3). The catalogue of CBMs proposed in the UN GGE 2015 report supplements the consensus achieved in the Organization for Security and Co-operation in Europe (OSCE)[39] and, even though not formally adopted by governments, remains the most comprehensive set of such measures to date. It provides a framework that can be adapted by regional organisations taking into account their specific regional context.

---

31 United Nations, General Assembly resolution 53/70, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/53/70 (4 January 1999), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70.

32 United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/58/373 (17 September 2003), https://ccdcoe.org/sites/default/files/documents/UN-030917-ITISreply.pdf.

33 United Nations, General Assembly resolution 58/32, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/58/32 (18 December 2003), https://ccdcoe.org/sites/default/files/documents/UN-031208-ITIS_0.pdf.

34 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/60/202 (5 August 2005), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement.

35 United Nations, General Assembly, *Group of Governmental Experts*, A/65/201.

36 United Nations, General Assembly, *Group of Governmental Experts*, A/68/98.

37 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 (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.

38 United Nations, General Assembly, *Group of Governmental Experts on Developments*, A/70/174.

39 Many of the experts representing states in the UN GGE are also involved in the negotiations of the CBMs in the framework of the OSCE.

4.2 Organization for Security and Co-operation in Europe

Despite its diverse membership, with 57 states from Europe, North America and Asia, OSCE has been spearheading the only project formally endorsed by states aimed at development and implementation of CBMs. The need to address cyber security concerns was recognised for the first time in the OSCE declarations and resolutions adopted in 2008 in Astana,[40] and in 2010 in Oslo.[41] The 2011 Belgrade Declaration called on the international community 'to increase cooperation and information exchange in the field of cyber security, to agree on specific measures to counter the cyber threat and to create, where possible, universal rule of conduct in cyberspace'.[42] In 2012, the OSCE Permanent Council decided to establish an open-ended and informal OSCE working group tasked with elaboration of 'a set of draft confidence-building measures to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs'.[43]

The first meeting of the OSCE's Informal Working Group on CBMs related to ICT (IWG-CBM) was convened under the chairmanship of the United States (US). The meeting focused on over 50 proposals for CBMs put forth by various participating states.[44] A short paper presented by the chair focused on three main types of measures: a) enhancing basic confidence and predictability through transparency- and confidence-building measures; b) co-operative methods of crisis prevention and resolution in the event of discrete disruptive activities of non-state actors; and c) stability measures where participating states refrain from destabilising activities in cyberspace and engage in stabilising behaviour. A proposal for a Ministerial Council decision on CBMs to reduce the risks of conflict stemming from the use of ICT was tabled at the 2012 Ministerial Council in Dublin but no decision was adopted due to Russia's objections. Following this failure, the Istanbul Declaration of 2013 urged the OSCE to 'develop confidence-building measures to reduce the risk of cyber conflicts and to promote a culture of cyber security'.[45] On the basis of this political guidance, the OSCE launched the process aimed at the adoption of a set of CBMs. A historical compromise on a set of eleven voluntary CBMs in

40 'Astana Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Seventeenth Annual Session' (Organization for Security and Co-operation in Europe, Seventeenth Annual Session, Astana, 29 June to 3 July 2008), https://ccdcoe.org/sites/default/files/documents/OSCE-080703-AstanaDeclarationandResolutions.pdf.

41 'Oslo Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Nineteenth Annual Session' (Organization for Security and Co-operation in Europe, Nineteenth Annual Session, Oslo, 6-10 July 2010), https://ccdcoe.org/sites/default/files/documents/OSCE-100710-OsloDeclarationandResolutions.pdf.

42 'Belgrade Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Twentieth Annual Session' (Organization for Security and Co-operation in Europe, Twentieth Annual Session, Belgrade, 6-10 July 2011), https://www.oscepa.org/documents/all-documents/annual-sessions/2011-belgrade/declaration-4/3024-belgrade-declaration-eng/file.

43 'Decision No. 1039: On development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,' PC.DEC/1039 (Organization for Security and Co-operation in Europe, Permanent Council, 909th Plenary Meeting, 26 April 2012).

44 'Follow-Up on Recommendations in the OSCE PA's Monaco Declaration: Final Report for the 2013 Annual Session' (Organization for Security and Co-operation in Europe, General Committee on Political Affairs and Security, 2013), https://www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/follow-up-report-3/1782-2013-annual-session-follow-up-final-report-1st-committee-english/file.

45 Istanbul Declaration and Resolution Adopted by the OSCE Parliamentary Assembly at the Twenty-Second Annual Session (Organization for Security and Co-operation in Europe, Twenty-Second Annual Session, Istanbul, 29 June to 3 July 2013), https://www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/declaration/1801-istanbul-declaration-eng-1/file.

Table 2. Linking norms, CBMs and capacity-building.[46]

NORMS	
Norms, rules and principles of responsible behaviour (UN GGE 2015 Report)	**Challenges to implementation**
In case of ICT incidents, states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.	Highly dependent on political agenda and uncertainty. CBMs are useful tools in creating 'positive expectations' and good faith where doubts exist.
States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.	Proving if a country has known about such acts from their territory is difficult. CBMs help to determine if this is the case.
States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.	Such cooperation is usually based on law enforcement cooperation treaties and relatively easy to monitor. Political will might be an obstacle to implementation that needs to be addressed with CBMs.
States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as UNGA resolutions 68/167 and 69/166 on the right to privacy in the digital age.	Relatively easy to verify with regard to freedom of expression but more complicated with regard to protection of privacy online. CBMs can help improve overall climate for cooperation.
States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.	This statement leaves untouched activities by non-governmental entities of which governments may be aware but not actively support. CBMs can help clarify state's position and demonstrate good faith.
States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account UNGA resolution 58/199 on the creation of a global culture of cyber security and the protection of critical information infrastructures, and other relevant resolutions.	Some countries may not have resources to implement concrete legal or technological solutions and be more vulnerable. In such cases capacity-building amounts to an important CBM.
States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.	In practical terms, such requests can be subjected to extended wait-times and undermine position of the addressee country. CBMs can help clarify reasons for possible delays or missing information.
States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.	These are often difficult to verify. CBMs like export controls and transparency measures – including cooperation among private sector – can be useful way for diffusing potential tensions.
States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.	These are relatively easy to implement through CBMs, if there is enough political will. CBMs at operational level can be more successful.
States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams of another State. A State should not use authorised emergency response teams to engage in malicious activity.	May be difficult to prove and hence CBMs – both at political and operational level – can help clarify the context and resolve conflicts.

46 Author's compilation on the basis of 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures,' PC.DEC/1106; United Nations, General Assembly, *Group of Governmental Experts*, A/70/174.

		CONFIDENCE-BUILDING MEASURES	CAPACITY-BUILDING
		Applicable measures (UN GGE 2015 and OSCE)	**Corresponding capacity-building needed**
	Facilitating cooperation	· Facilitation of cooperation between relevant national bodies (OSCE and UN GGE)	· Competent institution responsible for cyber security policy · Establishing clear division of labour within national administration
	Improving situational awareness	· Sharing information on national organisation, strategies, policies and programmes (OSCE and UN GGE) · Providing a list of national terminology and definitions related to ICT security (OSCE)	· National cyber security strategy and legislation · Cyber procedures: technical, administrative and procedural measures to protect systems · Public-private partnerships
	Protection of critical ICT infrastructure	· Consultations to prevent political and military tensions and protect critical national ICT infrastructure (OSCE and UN GGE) · Sharing information on categories of infrastructure considered critical and facilitating cross-border cooperation to address their vulnerabilities (UN GGE)	· Risk assessment · Developing standards · Public-private partnerships
	Fight against cyber crime	· Put in place modern and effective legislation to facilitate cooperation and effective cross-border cooperation to fight cyber crime and terrorist use of ICTs (OSCE)	· Substantive and procedural laws, criminalisation of certain acts, respect for fundamental freedoms · Sustainable and scalable training for law enforcement, judges and prosecutors · Forensics · Formal and informal channels of communication
	Building resilience	· Providing contact data of existing national structures that manage ICT-related incidents (OSCE and UN GGE) · Development of focal points for the exchange of information on malicious ICT use and provision of assistance in investigations (UN GGE)	· Computer Emergency Response Teams (CERTs) · 24/7 points of contact · Common protocols for sharing information regarding cyber events

cyberspace was contained in Decision 1106 adopted in December 2013 (see Table 3).[47] Participating states may inquire about individual submissions by direct dialogue with the submitting state or during meetings of the Security Committee and IWG-CBMs.

The OSCE 'master plan' is implemented in three stages:

- *Adoption of transparency measures* such as establishing crisis communication mechanisms, and promoting diligence and resilience, as well as exchange of information about national policies and structures. To date, around 40 participating states have implemented one or more of the CBMs adopted in OSCE Decision 1106.[48] Most actions have been focused on sharing information about approaches to cyber security, national cyber and ICT security architectures and international engagement linked to agreed measures.
- *Development of cooperative measures* like assistance in building resilience and other capacity-building initiatives that would strengthen the collective capacity to deal with the cyber threat. Such measures might focus on the development of national security strategies, assistance with establishing Computer Emergency Response Teams (CERTs), or putting in place effective legislation. According to the officials involved in the process, Russia has raised reservations on a number of issues raising the argument that the mandate of the OSCE does not include capacity-building. Contrary to initial expectations, the 21st OSCE Ministerial Council held in December 2015 has failed to reach a compromise on the language, and negotiations over the second set of CBMs will continue throughout 2016 during the German Chairmanship of OSCE.
- *Adoption of stability measures* focused on strengthening states' commitment to refrain from certain types of destabilising activities. Observers agree that this stage will be most difficult to complete as it involves a high level of trust and commitment between the participating states.

As part of the process, the Swiss and Serbian OSCE Chairmanships hosted several workshops on the issue with the aim to take stock of the implementation of the adopted measures, to support the negotiation of a second set of CBMs, and to provide a platform for discussion between non-governmental stakeholders such as critical infrastructure operators. On the basis of the recommendations of the Swiss Showcase Event 2014, OSCE managed to advance the implementation of Decision 1106, in particular with regard to ensuring appropriate channels for consultation, building a network of cyber focal points, and expanding cooperation in the framework of the CBM process to other stakeholders.

47 '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.

48 Michele Coduri, speaker, 'Session I – Promoting the Implementation of the First Set of CBMs' (OSCE Chairmanship Event on Effective Strategies to Cyber/ICT Security Threats, Belgrade, 29-30 October 2015).

4.3 ASEAN Regional Forum

The ASEAN Regional Forum (ARF) is one of the main forums for the discussion of CBMs in Asia.[49] In 1995, ARF presented a Concept Paper which envisaged three stages of security cooperation: confidence-building, preventive diplomacy, and conflict resolution.[50] The proposed measures focused on two main areas: a set of principles to ensure a common understanding and approach to interstate relations in the region (i.e. dialogues on security perceptions, publication of white papers); and adoption of comprehensive approaches to security. In 2012, the Ministers of Foreign Affairs adopted the Statement on Cooperation in Ensuring Cyber Security that tasked ARF to promote dialogue on confidence-building, stability, and risk reduction measures among its members.[51] In the Chairman's Statement of the 21st ARF Ministerial Meeting in 2014, ARF was mandated to develop a work plan on ICT security focusing on practical cooperation on CBMs. In support of the process, ARF organised a series of seminars on CBMs in cyberspace and other events focusing on broader issues, including cyber incident response.[52] The ultimate goal of these initiatives was to bring together various communities dealing with technology, security or Internet infrastructure.

The purpose of the Work Plan presented at the Ministerial Meeting in May 2015 is to 'promote a peaceful, secure, open and cooperative ICT environment and to prevent conflict and crises by developing trust and confidence between states in the ARF region, and by capacity building'.[53] The objectives included 'promoting transparency and developing confidence-building measures to enhance the understanding of ARF Participating Countries in the ICT environment with a view to reducing the risk of misperception, miscalculation and escalation of tension leading to conflict'.[54] It proposes establishing an open ended Study Group on Confidence Building Measures to submit consensus reports recommending CBMs to reduce the risk of conflict stemming from the use of ICT. It also suggests that reports should draw on previous ARF discussions and relevant work in other regional and international forums. Looking at the proposals of concrete workshops to be organised in support of the Study Group, it is difficult to avoid the impression that they clearly build on

49 ARF brings together 27 states, including ten members of the ASEAN, ten ASEAN dialogue partners (EU, China, US, Russia, Japan, Australia, Canada, New Zealand, India, and South Korea), and DPRK, Mongolia, Pakistan, Timor-Leste, Bangladesh, Sri Lanka and Papua New Guinea (observer).

50 Amitav Acharya, *The ASEAN Regional Forum: Confidence-Building: Draft Report*, PWGSC Contact 041.08011-6-1610/01-SS (1997), http://www.amitavacharya.com/sites/default/files/ASEAN%20Regional%20Forum-Confidence%20Building.pdf.

51 'Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security' (ASEAN Regional Forum, 19th ARF, 2012), http://www.mofa.go.jp/files/000016403.pdf.

52 The workshops and seminars focused on: 'ARF Seminar on Confidence-Building Measures in Cyberspace' (Seoul, 11-12 September 2012), 'ARF Workshop on Cyber Confidence Building Measures' (Kuala Lumpur, 25-26 March 2014), 'ARF Workshop on Space Security' (Hoi An, 6-7 December 2012), 'ARF Workshop on Cyber Incident Response' (Singapore, 6-7 September 2012), 'ARF Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects' (Beijing, 11-12 September 2013) and 'ARF Workshop on Cyber Security Capacity Building' (Beijing, 29-30 July 2015): See Asean Regional Forum, 'List of ARF Track I Activities (By Inter-Sessional Year from 1994 to 2015),' http://aseanregionalforum.asean.org/library/arf-activities.html?id=582.

53 'ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies' (ASEAN Regional Forum, 7 May 2015), http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf.

54 Ibid.

Table 3. Summary of UN GGE and OSCE CBMs.[55]

UN GGE 2013 Report and UN GGE 2015 Report recommendations	OSCE Decision 1106
Communication and information exchange	
· The creation of bilateral, regional and multilateral consultative frameworks for confidence-building, which could entail workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from State use of ICTs and how these incidents might develop and be managed; · Enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms; · Exchanges of information and communication between national CERTs bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels; · States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders, through: - Creating a repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of relevant related materials deemed appropriate for distribution; - Development of mechanisms and processes for consultations; - Development of technical, legal and diplomatic mechanisms to address ICT-related requests; - National arrangements to classify ICT incidents in terms of the scale and seriousness.	· Provide national views on various aspects of national and transnational threats to and in the use of ICTs. Facilitate co-operation among the competent national bodies and exchange of information; · Provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level; · Exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs; · Use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats; explore further developing the OSCE role in this regard; · Nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs; Update contact information annually and notify changes no later than thirty days after a change has occurred; · At the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs.

55 Author's compliation on the basis of 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures,' PC.DEC/1106; United Nations, General Assembly, Group of Governmental Experts A/68/98; United Nations, General Assembly, Group of Governmental Experts, A/70/174.

Transparency and verification	
· Identification of points of contact at the policy and technical levels to address serious ICT incidents and creation of a directory of such contacts; · Development of and support for mechanisms and processes for consultations to reduce risks of misperception, escalation and conflict; · Encouraging transparency by sharing national views and information on national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; CBMs developed in regional and multilateral forums; and relevant national organisations, strategies, policies and programmes; and · Provision of national views of categories of infrastructure considered as critical and national efforts to protect them, including national laws and policies for the protection of data and ICT-enabled infrastructure.	· Hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict, and to protect critical national and international ICT infrastructures including their integrity; · Share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet; · Share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; and · As a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. In the longer term, participating States will endeavour to produce a consensus glossary.
Cooperative measures of non-military nature	
· Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile state actions; · Cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions; · Cooperation, including the development of focal points for the exchange of information on malicious ICT use and assistance in investigations; · Creation of a national CERT/CSIRT or officially designating an organisation to fulfill this role. States should support and facilitate the functioning of and cooperation among such national response teams and other authorised bodies; · Expansion and support for practices in CERT/CSIRT cooperation, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organising exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation; and · Cooperation, in a manner consistent with national and international law, with requests from other states in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.	· Put in place – if they so decide – modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, in order to counter terrorist or criminal use of ICTs.

the OSCE set of CBMs. The workshops are supposed to explore the feasibility and possible modalities for:

- Voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations on security of and the procedures for information sharing;
- Table-top exercises on preventing ICT-related incidents that may evolve into regional security problems;
- Development of rules, norms, and principles of responsible behaviour and the role of cultural diversity in the use of ICTs;
- Measures to promote cooperation against criminal and terrorist use of ICTs including, cooperation between law enforcement agencies and legal practitioners, possible joint task force between countries, crime prevention and information sharing on possible regional cooperation mechanism;
- Terminology related to ICT security to promote understanding of different national practices and usage;
- Establishment of senior policy points of contact to facilitate real time communication about events and incidents of potential regional security significance; and
- Establishment of channels for online information sharing on threats in ICT, global ICT incidents, and sources of ICT attacks threatening critical infrastructure, and development of modalities for real time information sharing.

Even though these are not framed as CBMs in the strictest sense, they bare clear resemblance to measures developed by the OSCE. Also, since finding compromises within ARF has become complicated given its expanding membership, including actors like the EU, US, China and Russia, it is not surprising that without a strong tradition of multilateral cooperation in the region, the ARF members have opted to first explore the feasibility of certain options. While reaching consensus on concrete measures is difficult due to the complicated relations between some members, different political systems, and levels of development, the intermediate results of the OSCE process might be particularly helpful in identifying measures on which states are most likely to cooperate.

4.4 Organization of American States

The Organization of American States (OAS) launched its efforts to develop CBMs at the First Summit of the Americas in 1994. The Plan of Action adopted at the summit expressed support for actions that encourage regional dialogue and strengthen mutual confidence.[56] OAS also held two regional conferences on confidence- and

56 'Summit of the Americas Plan of Action' (Organization of American States, First Summit of the Americas, Miami, Florida, 9-11 December 1994), http://www.summit-americas.org/miamiplan.htm.

security-building measures in Santiago[57] (1995) and San Salvador[58] (1998) resulting in development of two comprehensive sets of CBMs, including adoption of agreements regarding advance notice of military exercises and exchange of information on defence policies and doctrines.

With an increasing need to address security challenges that could undermine developmental gains stemming from the use of ICTs, the 2002 meeting of the Committee on Hemispheric Security of the Permanent Council addressed the security of critical information systems and considered the need to develop a cyber security strategy. In 2004, OAS adopted the Comprehensive Inter-American Cybersecurity Strategy with an overall aim to foster 'a culture of cyber security that deters misuse of the Internet and related information systems' and encourage 'the development of trustworthy and reliable information networks'.[59] The strategy encompasses a number of initiatives aimed at strengthening trust and confidence in cyberspace, including:

- Formation of an inter-American alert, watch, and warning network to rapidly disseminate cyber security information and respond to crises and incidents;
- Addressing trust issues as an essential element of the hemispheric network in order to create the right environment for CSIRTs to exchange proprietary or otherwise sensitive information. This could be achieved through developing a secure infrastructure for managing sensitive information, enhancing the ability to communicate securely with stakeholders, and establishing procedures to guard against inappropriate disclosure of information;
- Identification and adoption of technical standards for a secure Internet architecture; and
- Building up legal capacities of OAS member states to protect Internet users and information networks. Concrete measures mentioned in the strategy include drafting and enacting effective cyber crime legislation and improving international handling of cyber crime matters.[60]

57 'Declaration of Santiago on Confidence- and Security-Building Measures' (Organization of American States, Regional Conference on Confidence- and Security-Building Measures, Santiago, 8-10 November 1995).

58 'Declaration of San Salvador on Confidence- and Security-Building Measures' (Organization of American States, Regional Conference on Confidence- and Security-Building Measures, San Salvador, El Salvador, 25-27 February 1998), http://www.oas.org/csh/english/csbmdeclarsansal.asp.

59 'Adoption of A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity' (Organization of American States, Fourth Plenary Session, 8 June 2004), http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

60 'Adoption of A Comprehensive Inter-American Cybersecurity Strategy'.

The OAS experience is noteworthy since it has taken a different approach to other regions by resorting directly to the development of cooperative measures. For instance, OAS members have made concrete commitments to step up cyber crime and infrastructure protection cooperation. Since the adoption of the strategy, cooperation between responsible national authorities such as Computer Emergency Response Teams and law enforcement agencies has improved consistently with regard to information sharing and technical cooperation. At the same time, the region exhibits imbalances with regard to cyber-related development; while some countries have advanced their technical and investigative capabilities and have in place requisite laws, others still grapple with meeting basic needs such as setting up a CERT or passing cyber crime legislation.[61]

5. Trends in Development of CBMs

As the overview of existing confidence-building initiatives suggests, there is no 'one-size fits all' approach. This stems from different historical and political contexts within which regional organisations operate and differences in their respective powers and decision making procedures. It is therefore important to highlight that the starting point is not the same for everyone: whereas the OSCE was able to draw from its decades-long experience with CBMs, the ASEAN Regional Forum approach is pragmatic and action oriented, including organising seminars and workshops in order to explore the possibility of establishing similar measures in the future.

Despite those differences, it is possible to identify two major trends in the debate about the future development of CBMs. A first trend – broadening the scope of CBMs – describes an increasing focus on building states' cyber capacities to ensure that all countries meet certain baseline levels of capacities that would enable them to participate in the development and implementation of CBMs. That also implies bringing in new actors, including the private sector, utility managers, and academic institutions. A second trend – deepening of CBMs – addresses the proliferation of bilateral cyber pacts between states in order to supplement norms and CBMs developed regionally and internationally with more politically binding arrangements. These quasi-agreements are viewed as a way to provide additional guarantees that their signatories will behave responsibly in cyberspace.

5.1 Broadening Cooperation Through Capacity-Building

The discussion about norms of behaviour and CBMs assumes that states possess a certain level of capabilities that allows them to participate in the implementation of concrete CBMs. For instance, a state which does not have a cyber security strategy

61 Symantec, Organization of American States, *Latin America+Caribbean Cyber Security Trends Report* (June 2014), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OAS-Symantec_Cyber_Security_Report_2014.pdf.

or a functioning CERT will not be able to exchange information about structures in place or contribute to management of specific incident. In that respect, the lack of participation may in some instances be interpreted as hostility. The UN GGE 2015 report explicitly acknowledged the link between compliance with norms and capacity of developing countries. While recognising that decision makers, in particular politicians, military staff and diplomats, are the primary addressees of the CBMs, one cannot ignore the fact that in order to take informed decisions, they need to rely on and interact with technical experts, law enforcement agencies and the private sector.

The scope of the existing challenges and the variety of financial and human resources needed to address them, require framing development of CBMs as a multi-level and multi-stakeholder engagement involving all parts of government and the private sector. Given that protection of ICT-enabled infrastructure and adequate response capacities in case of attacks is evolving into one of the main norms of behaviour in cyberspace, cooperation models among the incident respondents' community emerges as one of the key confidence-building elements. Various models of cooperation are already in place and could be increasingly involved in CBMs, ranging from assistance in establishing national CERTs[62] to bilateral team-to-team cooperation.[63] For instance, FIRST is a global 'trust network' composed of more than 300 computer security incident response teams from the public and private sectors.[64] FIRST strengthens trust within the global incident response community by fostering coordination in incident prevention and response, as well as by promoting information sharing among members. Similar venues have been established at the regional level, including AP-CERT[65] for Asia Pacific and AfricaCERT[66] for improving cooperation among African countries.

Certain steps were also made towards building and strengthening law enforcement and judicial capacities of countries in need of assistance, including through developing adequate legal frameworks, training of law enforcement officials, and strengthening cyber forensic capacities.[67] With regard to law enforcement cooperation, UN General Assembly Resolution 55/63 of 2001 calls on states to prevent their territories from being used as safe havens and to cooperate in the investigation and prosecution of international cyber attacks.[68] Similarly, the efforts undertaken in the framework of the Council of Europe Convention on Cybercrime – the only international legally binding treaty on the fight against cyber crime – are worth mentioning.[69]

62 Deloitte Bedrijfsrevisoren and Lionel Ferette, European Union Agency for Network and Information Security, 'Supporting the CERT Community "Impact Assessment and Roadmap"', Ver. 1.0 (1 December 2014), https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap.

63 European Union Agency for Network and Information Security, 'CERT Cooperation and Its Further Facilitation by Relevant Stakeholders,' Deliverable WP 2006/5.1(CERT-D3) (2006), http://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders.

64 FIRST, www.first.org.

65 APCERT, www.apcert.org.

66 AfricaCERT, www.africacert.org

67 European Union, Council of Europe, *Capacity Building on Cybercrime*: *Discussion Paper* (1 November 2013), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6.

68 United Nations, General Assembly resolution 55/63, *Combating the Criminal Misuse of Information Technologies*, A/RES/55/63 (22 January 2001), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

69 Council of Europe, *Convention on Cybercrime: CETS No. 185* (Budapest, 2001), http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

Some countries and international actors have also established bilateral venues for cooperation. The EU, for instance, has established a number of dialogues with third countries to enhance cooperation in the fight against cyber crime.[70] In September 2015, the US and China agreed to establish a 'high-level joint dialogue mechanism on fighting cyber crime and related issues'. The dialogue will focus on concrete confidence-building measures such as review of the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side; establishing a hotline for the escalation of issues that may arise in the course of responding to such requests. Both sides also agreed to cooperate with requests to investigate cyber crimes and provide updates on the status and results of those investigations, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory.

5.2 Deepening Cooperation Through Bilateral Agreements

In recent years, states have also increasingly opted for entering into bilateral agreements – either as formal international treaties or more informal political arrangements – in cases where the limited trust needed to be compensated with additional verification and enforcement mechanisms. The examples of such agreements include:

- *US-Russia agreement.* In June 2013, the US and Russia signed a landmark agreement to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern.[71] The US-Russia pact foresees the establishment of a hotline as one of the components in the existing Direct Secure Communication System between the White House and the Kremlin, and the exchange of technical information between the US Computer Emergency Response Team and its Russian counterpart. To avoid any risk of misperception and escalation, both sides agreed to expand the role of the Nuclear Risk Reduction Centre established in 1987 to exchange information about planned cyber exercises or cyber incidents.
- *Russia-China agreement.* In May 2015, Russia and China concluded a non-aggression agreement by virtue of which both sides agreed to refrain from cyber attacks against each other and to jointly respond to technologies that may have a destabilising effect on political and socio-economic life or interfere with the internal affairs of the state.[72]

70 Patryk Pawlak, *Cyber diplomacy: EU Dialogue with Third Countries: Briefing* (European Parliamentary Research Service, June 2015), http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI%282015%29564374_EN.pdf.

71 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.

72 See Olga Razumovskaya, 'Russia and China Pledge Not to Hack Each Other,' *Wall Street Journal*, May 8, 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/; Andrew Roth, 'Russia and China Sign Cooperation Pacts,' *New York Times*, May 8, 2015, http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html.

- *US-China agreement*.[73] Announced during President Xi Jinping's visit to Washington in September 2015, this agreement expresses in clear terms the both parties' commitment to the some of the peace-time norms outlined in the 2015 UN GGE report. Both sides have agreed to a number of CBMs, including to provide one another with a timely response to requests for information and assistance concerning malicious cyber activities, and to refrain from conducting or knowingly-supporting cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors.[74] Speaking of the 'consensus' reached between China and the US, Foreign Ministry spokesperson Hong Lei said that it 'will help enhance mutual trust and promote cooperation between the two countries in this regard, and have positive effects on the sound and steady growth of China-US relations.'[75]

Since public knowledge about the content of these agreements is limited to information provided in press releases and official statements, it is hard to assess their impact on the development of CBMs. It is fair to assume, however, that since most disagreements exist on Washington-Moscow-Beijing axis, any agreements reached between the representatives of these countries are likely to shape the future development of confidence-building measures. At the same time, the lack of transparency surrounding these agreements, while supposedly improving the relations between their signatories, may create suspicion and diminish confidence of those not directly involved.

6. Stability in Cyberspace: What Future Role for CBMs?

The analysis presented in this chapter confirms the importance which international and regional organisations attach to the development of CBMs. This is not surprising given the potential negative impact that misunderstanding and miscalculation in cyberspace might have on international stability. Development of CBMs has been so far closely associated with the process of establishing norms of behaviour in cyberspace as a means to reduce the risk of misunderstandings but also indirectly to ensuring a continuous monitoring of the commitments to which individual states have subscribed. This is achieved through specific measures focused on increasing

73 Two more general Memoranda of Understanding on Confidence Building Measures (CBMs) in the field of military relations were signed between China and the US in November 2014. The White House, Office of the Press Secretary, *Fact Sheet: President Xi Jinping's State Visit to the United States*, 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

74 Ibid.

75 Ministry of Foreign Affairs of the People's Republic of China, *Foreign Ministry Spokesperson Hong Lei's Regular Press Conference*, 28 September 2015, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1301373.shtml.

transparency and communication. At the same time, there is a growing realisation in policy circles that compliance with the commitments is linked to the question of capacities of individual states.

As the result, norms, CBMs and capacity-building emerge as three main pillars in the process of developing a sustainable and stable digital environment. Analysing the linkages between the three, it is possible to distinguish two distinct models for the role of CBMs within this process: a demand-driven model, whereby CBMs play a complementary role in the operationalisation of norms; and a supply-driven model whereby CBMs emerge as a consequence of cyber capacity development.

In the *demand-driven model* for secure and stable cyberspace (Figure 1) norms of behaviour in cyberspace (both non-binding and encompassed in the international law) provide the impulse for development of CBMs. As shown in Table 2, in order to ensure effective implementation of certain norms it is necessary to develop CBMs. At the same time, the scope of CBMs may require engaging in capacity-building activities as a way to ensure that certain benchmarks of human, institutional, technological or legal capacity are achieved, and allows a given state to actively participate in the implementation of the CBMs. That also implies that, with the progressing development of capabilities, there might be a need to redefine or agree supplementary norms. Realisation of this possibility is essential in order to ensure that decisions about capacity development contribute to more trusted and stable cyberspace rather than a potential cyber arms race. The OSCE approach, at least at this stage, seems to be following this logic.

In the *supply-driven model*, the impulse for development of CBMs is provided by progressing development of cyber capacities. This model is not very much present in the ongoing debates. This is understandable given that the discussion about norms is primarily the matter of state relations whereas cyber capacities are generated primarily by non-state actors (including the private sector, cyber criminals, and hackers). In the supply-driven model, CBMs are developed primarily to minimise the risks to delivery of services or products with the use of ICTs. This implies developing concrete cooperative CBMs between all stakeholders, including law enforcement agencies or technical communities. Norms are then developed with the primary objective to regulate the states use of the existing and future capabilities. To some degree, this model was much more dominant in the 1990s when the discussion about the peaceful use of ICT was initiated. It then evolved towards a more demand driven model. The OAS approach to developing confidence-building measures is probably the closest to this model in that it uses the capacity-building processes such as the support provided for setting up CERTs, cyber crime legislation, and cyber security strategies to almost simultaneously promote the development of CBMs including points of contact and CERT-to-CERT cooperation. The ARF approach is guided by a similar logic and driven by the analysis of the existing capacities that could provide the foundation for development of concrete CBMs. Another approach – not discussed at length in this chapter but nonetheless

worth mentioning – adopted in the framework of the Wassenaar Arrangements[76] in December 2013 foresees restrictions on exports of IP network surveillance systems and intrusion software[77] in order to prevent 'cyber proliferation'.[78] The restrictions were imposed, among others, on 'zero-day' exploits which are purchased by governments for the purpose of targeted attacks.[79]

Figure 1. Demand-driven model.

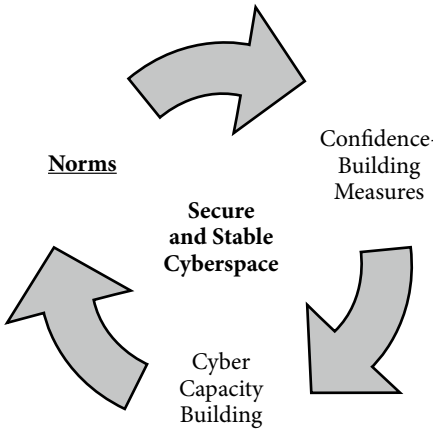
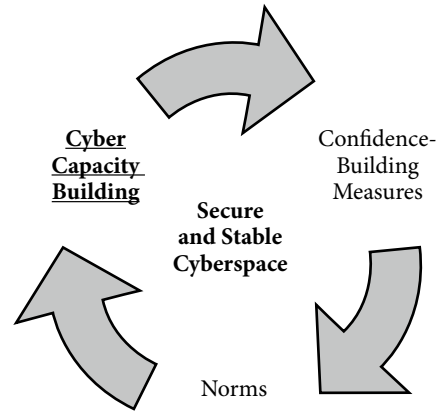


Figure 2. Supply-driven model.



These models, although definitely requiring further elaboration, allow drawing two main conclusions with regard to the future development of CBMs. First, understanding the underlying dynamic relationship between norms, CBMs, and capacity-building within the existing models is essential for building bridges between various regional approaches beyond those discussed in this chapter. For instance, the International Code of Conduct for Information Security promoted by the Shanghai Cooperation Organization recognises the need to develop CBMs aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict. This includes the voluntary exchange of information regarding national strategies and organisational structures, the publication of white papers

76 It is an international regime regulating exports of conventional weapons and sensitive dual-use items and technologies with military end uses. The participating states of the Wassenaar Arrangements are: all EU member states (except for Cyprus), Argentina, Australia, Canada, Japan, Mexico, New Zealand, Norway, South Korea, Russia, South Africa, Switzerland, Turkey, Ukraine, and US. See 'The Wassenaar Arrangement,' www.wassenaar.org.

77 Jennifer Granick, *Changes to Export Control Arrangement Apply to Computer Exploits and More* (Stanford Law School, The Center for Internet and Society, 2014), http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more.

78 Sam Jones, 'Cyber War Technology to be Controlled in Same Way as Arms,' *Financial Times*, December 4, 2013, http://www.ft.com/intl/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html#axzz3wSJjk22o.

79 Brian Fung, 'The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities,' *Washington Post*, August 31, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/.

and exchanges of best practice.[80] With the official aim to create more reliable and cooperative environment between its signatories, the Code had the opposite impact on relations with other members of the international community – notably European Union and the US – who expressed concern that some of the provisions in the document can be interpreted in a way that is not compatible with existing international law, and in particular human rights law. In a similar vein, the Communique issued in October 2015 by the BRICS countries highlights the need 'to promote measures and facilitate favourable conditions for ensuring the progressive development of ICTs … such as the equitable use of security measures relating to the continuity and stability of the use of ICTs in all spheres of life and production'.[81]

Second, it is crucial to understand the role of capacity-building in the development of CBMs and ensuring the stability of cyberspace in general. It is not to say that the process of capacity-building automatically leads to more unstable and unpredictable cyberspace. As a matter of fact, capacity-building projects implemented nowadays focus on using ICT to stimulate social development, human security and economic growth. Ironically, bringing the elements of capacity-building into the discussion about CBMs might also offer a solution to one of the main weakness of the existing CBMs; their voluntary nature and the absence of compliance verification mechanisms. By engaging with product designers or utility managers from the very beginning it might be possible to prevent certain undesired developments and enhance cooperation between those actors without a need for additional CBMs. This point is particularly important in light of the growing use of ICT platforms and a potential inability to continuously expand CBMs to those new policy areas.

7. Conclusion

The development of confidence-building measures is closely linked to the debate about norms in cyberspace. However, the examples from different regional organisations currently engaged in developing CBMs show that while norms help to establish certain benchmarks for responsible state behaviour, the difficulties with attributing certain acts and still nascent opportunities for verification call for defining alternative solutions that could help overcome limited trust and reduce the risks of misunderstandings. CBMs have emerged as one such alternative. Consequently, the chapter has focused on confidence-building processes within the UN

80 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.

81 'Communique of BRICS Ministers of Communications on the Outcomes of the Meeting on "Expansion of Cooperation in the Field of Communications and ICTs"' (Meeting of ICT Ministers of the BRICS group, Moscow, 23 October 2015), https://en.brics2015.ru/load/637860.

framework and at the regional level, including in the OSCE, OAS and ARF. A closer analysis of these processes points to the emergence of two overarching trends: an increasing significance of the capacity-building processes in order to help individual states meet their commitments, and assuring additional guarantees through bilateral agreements. This has led to the conclusion that norms, CBMs and capacity-building constitute three pillars on which stability in cyberspace needs to be constructed. Finally, looking at the drivers for development of CBMs, the chapter suggests that the ongoing efforts can be better understood through demand-driven and supply-driven models.

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

CHAPTER 8

Outer Space and Cyberspace: A Tale of Two Security Realms

Paul Meyer

International security policy has most often been a function of competition between sovereign states over divergent national interests. This competition is rooted in the requirement of the state to defend its national assets, including territory, people, resources and infrastructure, from encroachment by other states or external forces. This requirement leads in turn to the creation of armed forces and the other components of national security establishments in order to protect these sovereign assets. But what is the appropriate security posture to assume with respect to spaces beyond the claims of sovereign states and national appropriation? These spaces are comprised of the so-called 'global commons' which have been the subject of special regimes devised by sovereign states.[1] These regimes have recognised the importance of access to and use of the spaces concerned by states for a variety of security and economic ends, while sometimes granting them a distinctive status as a 'common heritage of mankind'.

1. Global Commons

The earliest example of such a space and a special regime applied to it was the maritime domain. The initial navigational accomplishments of Portugal and

1 For the evolution of this concept in international relations, I have relied especially on John Vogler, 'Global Commons Revisited,' *Global Policy* 3 (2012): 61-71.

Spain in the fifteenth and sixteenth centuries (unlike their terrestrial conquests) could not be translated into enduring control over the world's oceans. Other powers also wanted to exploit the new maritime routes and the only alternative to permanent conflict was to arrive at some generally acceptable governance of the seas. Building on the writings of the international legal pioneer Hugo Grotius, states gradually embraced his concept of an international maritime order which consisted of two parts: a territorial sea under exclusive sovereign control (which custom eventually set at three miles because that was the range of land-based cannons at the time) and the 'high seas' that were opened for common use and owned by none.[2] This construct has been largely upheld by states over the intervening centuries, and received its most comprehensive codification in the UN Law of the Sea Convention of 1982. There are two other environments to which access has only been possible much more recently and for which common understandings and international agreements are just beginning to emerge. These environments are becoming increasingly important for a range of security, commercial and scientific pursuits although their character under international law and the practice of states is only now being shaped. What international security order, if any, will be established for these two environments remains to be seen, but the expansion of access and use of both should act as a spur to states to agree on a common approach sooner rather than later.

The two environments in question are outer space and cyberspace (or, as some prefer it, 'information space'). In considering these realms from an international security perspective, one is struck by several key similarities, but also some significant differences between them. In policy terms, this article will argue that there is room in both 'spaces' for an exercise of preventive diplomacy and the development of Confidence-Building Measures (CBMs) and cooperative security. We will first review the parallels between the environments and then proceed to an examination of the differences including how well the 'global commons' designation applies to them. On the basis of this comparative analysis we can discuss the case for sustaining the present, essentially benign operating environment of the two spaces through a conscious policy of international security cooperation. This cooperation frequently develops through a continuum that begins with the expression of principles or norms for state conduct, proceeds through the elaboration of political arrangements or measures and culminates in binding international agreements. The chief diplomatic proposals that have been put forward to secure such cooperation in the space and cyber realms will be examined and the article will conclude with an assessment of the prospects for cooperation in these two special security realms.

2 John Ruggie, 'Multilateralism: The Anatomy of an Institution,' *International Organization* 46 (1992): 575.

2. The Similarities

The first similarity between outer space and cyberspace, beyond their relative vastness, is their 'global commons' character. In both cases the international community has acknowledged that these environments in some way belong to humanity and are beyond national appropriation. In the case of outer space, this 'global commons' status is explicitly set out in the foundational Outer Space Treaty of 1967. Article I of that treaty stipulates that the use of outer space 'shall be carried out for the benefit and in the interests of all countries … and shall be the province of all mankind'. Article II reinforces this concept of global ownership by specifying that outer space, including the moon and other celestial bodies, is 'not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means'.[3] With respect to cyberspace, this 'global commons' status is not as explicitly or legally set out as is the case with outer space, but a similar vision animates the pronouncements of states. The most authoritative of these statements to date were those agreed to by consensus at the UN-mandated World Summit on the Information Society (WSIS), which was held in two stages in Geneva and Tunis in 2003 and 2005 respectively. The Declaration of Principles adopted by WSIS described 'a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge … '.[4] More recently, through the results of a series of UN Group of Governmental Experts (GGE) meetings on 'Developments in the Field of Information and Telecommunications in the Context of International Security' the notion of cyberspace as a special realm to be used for the good of humanity and in a peaceful manner has also been advanced. The latest GGE report, for example, '[u]nderscor[es] the aspirations of the international community to the peaceful use of information and communication technologies (ICTs) for the common good of mankind'.[5]

Other analysts have suggested that the question of access is the defining characteristic of a commons. Within an international security perspective, national security actors have stressed the importance of maintaining free access to the global commons. Illustrative of this perspective and policy orientation are the pronouncements of the US national security establishment. In a policy document outlining defence priorities for the 21st century, the US Department of Defense declared: 'America, working in conjunction with allies and partners around the world, will seek to protect freedom of access throughout the global commons – those areas

3 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty)*, 10 October 1967, *United Nations*, http://www.nti.org/media/pdfs/aptospc.pdf?_=1316555222&_=1316555222.

4 First Phase of the World Summit on the Information Society, *Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/4-E (12 December 2003), para. 1, http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

5 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. 12, http://www.un.org/ga/search/view_doc.asp?symbol=A%2F70%2F174&Submit=Search&Lang=E.

beyond national jurisdiction that constitute the vital connective tissue of the international system'.[6] In a NATO document entitled *Assured Access to the Global Commons* the authors identify this commons as comprised of the four domains of maritime, air, space and cyber and assert that 'the security and prosperity of our nations, individually and for the Alliance as a whole, rely on assured access to and use of the maritime, air, space and cyberspace domains that are the commons'.[7] Another military writer has described cyberspace, the newest of the domains, as 'characterized by permeable physical, political and social boundaries and a cyber culture that vigorously resists state control … the cyber domain is available to all nations and regarded as part of the global commons'.[8]

The second similarity is that both outer space and cyberspace are currently being used to provide a wide array of services and benefits, overwhelmingly civilian in nature. Approximately 1,200 satellites are currently operating in outer space on behalf of 60 states or commercial consortia.[9] Space-based services are being used by consumers around the globe. The exploitation of cyberspace is even more extensive, with over three billion Internet users and an increasing penetration in the developing world, where the majority of users are now found.

The third common feature is that while military activity is present in both environments, and has been for several years, these environments have not yet been 'weaponised' or transformed into active battle zones. In this context, weaponisation means the general introduction into an environment of offensive arms capable of destroying or damaging objects within that same environment. Moreover beyond exercising restraint regarding the introduction of weapons, there is an evident direction on the part of states to maintain a peaceful character for these environments. Again the 1967 Outer Space Treaty is explicit in this regard with its preambular references to the 'use of outer space for peaceful purposes' and its prohibition on any deployment of weapons of mass destruction or military activity on the moon or other celestial bodies. The WSIS Declaration of Principles is more indirect in its espousal of a peaceful character for cyberspace, although this orientation can be inferred from its affirmation that 'the Information Society should respect peace …' and its call that '[a] global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders … '.[10]

A fourth commonality is that both spaces pose particular difficulties for the monitoring and verification of state behaviour. Although there is a large-scale effort to monitor outer space anchored in the US military-operated Space Surveillance Network, this is primarily directed at tracking space debris and avoiding collisions

6 Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, 2012), 3, http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf.

7 Mark Barrett, et al, *Assured Access to the Global Commons* (Norfolk: North Atlantic Treaty Organization, 2011), xii, http://www.alex11.org/wp-content/uploads/2013/01/aagc_finalreport_text.pdf.

8 Ian K. Adam, 'The Character of Conflict,' in *Conflict and Cooperation in the Global Commons:* A Comprehensive Approach for International Security, ed. Scott Jasper (Washington: Georgetown University Press, 2012), 45.

9 Cesar Jaramillo, ed., *Space Security Index 2014* (Canada 2014), 23, http://spacesecurityindex.org/wp-content/uploads/2014/11/Space-Security-Index-2014.pdf.

10 First Phase of the World Summit on the Information Society, *Declaration of Principles,* paras. 35, 56.

and is not geared towards verifying the state of space assets generally. Verification of any potential restrictions on military activity in space has been viewed as a difficult task, and one that, in the opinion of some, would render any eventual arms control measures in space unverifiable. An analogous situation pertains in cyberspace, in which the extent and nature of the technology employed poses major challenges for monitoring activity, making attribution and verifying compliance with possible cooperative arrangements challenging.

Finally, and probably linked to the last point, is that neither outer space nor cyberspace has been subjected to much in the way of international governance or regulation to preserve their peaceful character with the important early exception of the Outer Space Treaty. This limited governance presence is the current reality even as it is widely acknowledged that both environments would be highly vulnerable if destructive attacks were to occur in them. The Obama Administration's *National Security Strategy* stated for example: 'The space and cyberspace capabilities that power our daily lives and military operations are vulnerable to disruption and attack.'[11]

3. The Differences

In turning to the differences between the two spaces, the first and most obvious is that outer space is a natural environment whereas cyberspace is a human-made one. Outer space is a vast, timeless domain in which humankind is only gradually projecting itself. Cyberspace, while equally vast at one level, has been developed in the timeframe of a generation and its nature is purely within human control.

A second major difference between the two spaces might be described as the 'threshold of entry' to them. To enter and use outer space requires sophisticated and costly assets and capabilities, usually possessed by a small number of states and a few multinational companies. Cyberspace, by contrast, can be explored by anyone with a personal computer or mobile device. The basic equipment is relatively cheap and users are numbered in the billions.

A third difference between the realms is that outer space activity is still dominated by state actors although there is a recent trend towards privatisation of some services. Currently there are only ten spacefaring nations possessing an independent orbital launch capacity. In contrast, the infrastructure of cyberspace is largely owned and operated by the private sector and civil society.

Finally, there is a difference in the manner in which the two realms have been treated to date under international law. Outer space has benefited from an early

11 The White House. *National Security Strategy* (Washington, 2010), 8, https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

foundational treaty that defined its character. Although this treaty is now 48 years old and many states believe that the legal regime it created for outer space needs to be reinforced,[12] it nonetheless provides an authoritative reference point. No similar treaty has yet been devised to define cyberspace and efforts to formalise cooperation via international legal instruments such as the 2001 Budapest Convention on Cyber Crime have not as yet met with widespread support amongst states.[13]

4. External Drivers

Taking into account the results of this brief survey of the similarities and differences of the two environments of outer space and cyberspace, there are two preliminary conclusions to be drawn for the purposes of international security. The first is that the current benign environment for operating in outer space and cyberspace provides major benefits to the international community and should be preserved. The second is that this current benign condition should not be taken for granted and that states (and stakeholders) should engage diplomatically now in order to ensure that these unique spaces are indeed preserved for peaceful use by humanity in the future. Achieving this goal will require the forging of new agreements and the development of innovative measures of practical cooperation.

In the last few years, we have begun to witness the beginning of official efforts at the preventive diplomacy that this author would advocate for safeguarding both outer space and cyberspace. It would have been gratifying to have been able to attribute these initiatives to far-sighted and well-reasoned policies by key states. Regrettably, this recent activism was more likely prompted by external actions that threatened these long-standing benign environments which stirred governments into preparing some measures in an effort to forestall devastating consequences down the road.

For outer space, the disturbing events prompting government action were most probably the anti-satellite weapon (ASAT) tests carried out by China and the US in 2007 and 2008 respectively. The impact of these military actions, which raised the long dormant threat of ASAT employment, were exacerbated by the accidental collision of a defunct Russian satellite and an active American one in 2009 which further

12 See notably the resolution on the 'Prevention of an Arms Race in Outer Space' which is annually adopted by the UN General Assembly with near universal support and which in reference to the legal regime for outer space states that 'there is a need to consolidate and reinforce that regime and enhance its effectiveness …': United Nations, General Assembly resolution 69/31, *Prevention of an Arms Race in Outer Space*, A/RES/69/31 (11 December 2014), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/31.

13 The Convention developed by the Council of Europe has only been ratified or acceded to by 47 states of which only eight are non-member states of the Council of Europe, see *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.

contributed to the already disconcerting increase of space debris. Such debris, of course, poses a significant hazard for space operations and there are already warnings from informed observers that the build-up of such debris poses a constant and significant threat to all spacecraft, especially those in low earth orbit.[14]

For cyberspace, the external developments which seem to be spurring nascent diplomatic initiatives are the publicly revealed initiation of state-sponsored offensive cyber attacks in the form of the 'Stuxnet' and 'Flame' malware payloads, and the generally higher publicity being given to cyber attacks against a range of public and private institutions. Government agencies tend not to be forthcoming with their cyber attack statistics, but it is widely acknowledged that state institutions are far from being immune to penetrations of their computer networks and the exfiltration of sensitive data. Although the magnitude of attacks in cyberspace eclipse those in outer space, in both realms the diplomatic proposals now surfacing represent an effort by states to preclude destructive actions in these fragile environments and to promote a cooperative security approach with respect to them.

5. Diplomatic Proposals for Outer Space Security

The diplomatic proposals for outer space security that have been advanced consist of four main types. Russia and China have been developing for some time elements of a treaty that would prohibit the placement of weapons in outer space. The genesis of this effort can be traced back to 2002 when Russia and China first introduced a working paper at the Conference on Disarmament in Geneva presenting several elements for such a treaty. This initiative was probably in response to the decision by the United States the year before to abrogate the Anti-Ballistic Missile (ABM) Treaty and with it one of the few legally binding prohibitions on deployment of weapons in outer space (in this case, space-based ABM systems). China and Russia have developed these elements over the next years and in February 2008, a draft treaty 'on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects' (better known by its acronym PPWT), was formally presented at the Conference on Disarmament.[15] In essence this accord seeks to reinforce the Outer Space Treaty's prohibition on stationing WMD in outer space by extending this ban to all weapons in space. The draft met with criticism from several quarters. Some faulted its failure to address ground-based anti-satellite

14 Jaramillo, ed., *Space Security Index 2014*, 10.

15 See 'Possible Elements of the Future International Legal Instrument on the Prevention of Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects', CD/1679 (Conference on Disarmament, 28 June 2002), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G02/624/84/PDF/G0262484.pdf?OpenElement for the original China-Russia working paper and CD/1839 29 February 2008 and 'Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects', CD/1985 (Conference on Disarmament, 12 June 2014), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/050/66/PDF/G1405066.pdf?OpenElement for the draft PPWT.

weapons although given the inherent ASAT capability of ballistic missile interceptors, any effort to include ground-based systems would have run up against the US commitment to deploy ballistic missile defences. Other states complained about the lack of verification provisions for the treaty given the significant military prohibitions contained in it. The Chinese and Russian sponsors attempted to respond to these critiques and in June 2014 presented a revised version of the PPWT, which included a new article acknowledging the need for verification measures and suggesting that these could be elaborated in a subsequent protocol to the treaty. Whatever the merits of the draft text, further consideration of it has been stymied by the general blockage of the Conference on Disarmament and to date the treaty's sponsors have not decided to take their draft text to any other forum.

The second initiative was brought forward by the European Union, originally in December of 2008. It took the form of a 'Code of Conduct for Outer Space Activities' a politically-binding 'set of best practices' designed to support safe operations in space. While in many ways a re-packaging of existing commitments and principles regarding state activity in outer space, the Code does include provision for significant institutional support for the multilateral review of outer space activity via annual information exchanges, biennial meetings of subscribing states and a central 'point of contact' performing secretariat-like functions. The Code also foresees consultative mechanisms in the eventuality that activities are undertaken which could be contrary to the Code's commitments and which might pose a risk of damage to others. The EU has issued revised versions of its original proposal in 2010, 2012 and most recently in March 2014. Over this period the EU has conducted several bilateral and three multilateral consultations.[16] The EU's initial effort to confine consultations with others to bilateral tracks in a sort of 'hub and spoke' process was not well received, and important states such as China, India, South Africa and Brazil voiced concerns. The EU Code of Conduct initiative has also suffered from various disconnects and changes in responsible personnel and has experienced difficulty in maintaining diplomatic momentum for wider acceptance, despite an endorsement by the US in January 2012. EU representatives have indicated that they are ready to 'move the process from a consultation to a negotiating phase in an inclusive and transparent manner', but the exact way forward favoured by the EU is still unclear.[17] In July 2015 the EU, in cooperation with the UN Office of Disarmament Affairs, organised a session at UN HQ in New York that it hoped would constitute a multilateral negotiation of its draft Code and set the stage for its adoption. Several participating states, notably the BRICS grouping (Brazil, Russia, India, China and South Africa), opposed this approach insisting that the future elaboration of the Code be held 'in the format of inclusive and consensus-based multilateral

16 The most recent version is entitled European Union, *Draft International Code of Conduct for Outer Space Activities* (31 March 2014), http://www.eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_31-march-2014_en.pdf.

17 United Nations, *Speakers in First Committee Urge Balance of Conventional Forces in Hotbeds of Tension, Non-Militarization of Outer Space*, GA/DIS/3511, 27 October 2014, http://www.un.org/press/en/2014/gadis3511.doc.htm.

negotiations within the framework of the UN'.[18] It would seem in this light that any future negotiation of the EU's Code of Conduct would depend on seeking a resolution in the UN General Assembly to mandate such a multilateral process.

The third proposal was made by Canada in 2009 in the form of a working paper submitted to the Conference on Disarmament and reiterated in the context of the UN General Assembly.[19] This proposal consisted of a series of unilateral 'pledges' that would have states declare that they would not: test or use a weapon against a satellite so as to damage or destroy it; deploy any weapons in outer space; or use a satellite itself as a weapon. These commitments were seen as providing some of the security content missing in the EU Code while avoiding the problems associated with the PPWT's new treaty approach. Canada, however, has not actively promoted these ideas subsequently and other states have not come out in favour of them, although some concerned NGOs have suggested similar measures.[20]

The last initiative concerns the UN Group of Governmental Experts (GGE) that began its work in July 2012 pursuant to a Russian-led resolution that has been adopted for several years by the UN General Assembly.[21] The fifteen-member UN GGE was mandated to consider possible transparency and confidence-building measures for outer space, and produced a consensus report in the summer of 2013 that was presented to the General Assembly for consideration. The report described transparency and confidence-building measures as 'a means by which Governments can share information with the aim of creating mutual understanding and trust, reducing misperceptions and miscalculations and thereby helping both to prevent military confrontation and to foster regional and global stability'.[22] The report enumerated several potential transparency and confidence-building measures, including information exchange and notification, risk reduction measures, visits to space-related facilities, and consultative mechanisms. The report said that these transparency and confidence-building measures should be considered as non-legally binding voluntary measures and that they were 'neither a substitute nor a precondition for arms limitation and disarmament measures'.[23] Although the GGE was successful in producing a substantive report with specific recommendations for transparency and confidence-building measures, it could do no more than present this menu of potential action items to the international community and see if states were prepared to adopt the measures proposed.

18 United Nations, *BRICS Joint Statement Regarding the Principles of Elaboration of International Instruments on Outer Space Activities*, New York, 27 July 2015.

19 'On the Merits of Certain Draft Transparency and Confidence-Building Measures and Treaty Proposals for Space Security', CD/1865, (Conference on Disarmament, Canadian Government, 5 June 2009) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G09/615/92/PDF/G0961592.pdf?OpenElement.

20 Union of Concerned Scientists, *Securing the Skies: Ten Steps the United States Should Take to Improve the Security and Sustainability of Space* (November 2010), 18, http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/securing-the-skies-full-report-1.pdf.

21 United Nations, General Assembly resolution 65/68, *Transparency and Confidence-Building Measures in Outer Space Activities*, A/RES/65/68 (13 January 2011), http://www.unidir.org/files/medias/pdfs/general-assembly-resolution-eng-0-420.pdf.

22 United Nations, General Assembly, *Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities*, A/68/189 (29 July 2013), 12, http://www.unidir.org/files/medias/pdfs/outer-space-2013-doc-2-a-68-189-eng-0-580.pdf.

23 Ibid, 13.

One particular recommendation from the GGE that is due to be realised this fall is a joint session of the UN General Assembly's First and Fourth Committees, the committees that have dealt respectively with the security and peaceful uses of outer space themes. This special joint session, which is to address possible challenges to space security and sustainability, could provide a forum for focused consideration of the proposed transparency and confidence-building measures generated by the GGE. Regrettably the cooperative atmosphere that characterised the work of the GGE and contributed to its ability to fashion a consensus report has deteriorated in the post-2013 period, with the revival of East-West tensions over Ukraine that will render more difficult agreement on any new cooperative arrangements concerning outer space. Symptomatic of this current problematic diplomatic environment was the decision by Russia and several other states to push forward in 2014 with a new UN General Assembly resolution on 'no first placement of weapons in outer space' despite opposition from a significant minority of states. These states believed that declaratory commitments not to be the first to place weapons in outer space, as urged in the resolution, did not meet the criteria for true transparency and confidence-building measures as earlier agreed by the UN GGE. The sponsors decided nevertheless to proceed to a vote on the resolution, which was adopted with 126 states in favour, 4 opposed (Georgia, Ukraine, Israel and the US), and 46 abstaining. The divisive nature of this result was in contrast with the consensual status of most space-related resolutions in the General Assembly and reflects the gap that is opening up amongst space powers that may impede the adoption of any new cooperative agreements or arrangements in the near term.

6. Diplomatic Proposals for International Cyber Security

Diplomatic proposals for international security in cyberspace are more recent and less numerous than for outer space, but are also starting to surface. The US, while not bringing forward any specific proposal of its own, officially called for the forging of a consensus on 'norms for responsible state behaviour' in its path-breaking *International Strategy for Cyberspace* released by the White House in May 2011.[24] Having issued this important call for an urgent dialogue amongst states to develop these norms, the Obama Administration has found it difficult to translate this policy aim into any multilateral diplomatic process to yield the desired result. In the event, other states were the first off the mark in proposing some specific content to meet the goal of 'norms for responsible state behaviour'. In September of that year, Russia and China (in conjunction with Tajikistan and Uzbekistan) circulated

24 The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), 8, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

at the UN General Assembly a proposal for an 'International Code of Conduct for Information Security'. In presenting the proposal, Ambassador Wang Qun of China, declared that 'countries should work to keep information and cyberspace from becoming a new battlefield, prevent an arms race in information and cyberspace and settle disputes on this front peacefully through dialogue'.[25]

Originally, the key commitment of this voluntary code would be for states 'not to use Information and Communication Technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies'.[26] After having carried out consultations with other states on the margins of the UN General Assembly, China and Russia decided to issue a revised version of their Code of Conduct in January 2015. Significantly, the arms control orientation of the initial draft has been dropped in favour of a much more general formulation by which subscribing states would commit 'not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security'.[27] Presumably the consultations with others had persuaded the sponsors that the original arms control orientation was not feasible at this stage given the practical problems associated with it such as the lack of any agreed definition of an 'information weapon'. The revised Sino-Russian Code still retains a 'security' focus, however, especially in the elements aimed at countering content from information and communications technologies that is perceived to incite 'terrorism, separatism or extremism … [or threaten states'] … political, economic and social security'.[28] These provisions are aligned with Sino-Russian views on the necessity to police content and on the sovereign rights of states to exercise control over their information infrastructure. The very term 'information security' preferred by China and Russia to the term 'cyber security' favoured by the West is illustrative of the former's concern with content as opposed to the latter's focus on system integrity.

Diplomatically, the Sino-Russian partnership on new approaches to outer space security has carried over into cyberspace with a similar leadership being shown by Beijing and Moscow on arrangements to promote 'information security'. Their activism on the space and cyber security files also reflects a pragmatic capacity to refine their proposals in light of the prevailing diplomatic context. For example, the Russian-Chinese decision to present their set of cyber security norms as a voluntary, politically binding Code of Conduct instead of as an international legal instrument

25 Wang Qun, 'Work to Build a Peaceful, Secure and Equitable Information and Cyber Space' (Statement made at the First Committee during the 66th session of the General Assembly, New York, 20 October 2011), http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

26 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://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

27 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), 5, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

28 Ibid.

suggests that they had absorbed the lessons from their earlier joint initiative of the PPWT. With respect to the new cyber initiative the co-sponsors were opting now for a simpler format and one which would be easier and quicker for states to adopt. Russia and China as chief sponsors of this proposal have also proceeded with some care and have taken the time to conduct consultations with other states regarding their draft Code of Conduct, thus enabling them to present their revised version as reflecting input received from others. Arguably this has increased the eventual acceptability of their proposal for a Code of Conduct on Information Security and positions China and Russia to press for the adoption by the UN General Assembly of their text when they judge the time is propitious to do so.

One reason why Russia and China have decided not to move forward more rapidly with their draft Code of Conduct may be linked to the other major diplomatic initiative related to international cyber security that is currently on-going within the UN context. This is the work of the UN Group of Governmental Experts (GGE) on 'Developments in the Field of Information and Telecommunications in the Context of International Security' referred to earlier. These UN GGEs originated with a Russian-led UNGA resolution and first yielded a consensus report in 2010. The 2010 report observed that states were developing Information and Communications Technologies (ICTs) 'as instruments of warfare and intelligence' and called for 'confidence-building, stability and risk reduction measures to address the implications of state use of ICTs'.[29] Following close on the earlier report, another UN Group of Governmental Experts also got underway in the summer of 2012 and succeeded in producing a report in June 2013. The 2013 GGE report went further than its predecessor to warn that 'the absence of common understandings on acceptable State behaviour with regard to the use of ICTs increases the risk to international peace and security'.[30] The report recommended that states consider taking action on norms and principles of responsible behaviour, on confidence-building measures, and on capacity-building measures. Again while the GGE produced a set of practical if modest measures for states to consider, actual implementation is essentially left to the initiative of those states. Having already been instrumental in the establishment of the 2010 and 2013 GGEs, Russia decided to maintain the diplomatic momentum it had generated on the issue of international cyber security by initiating yet another GGE. This expanded GGE (20 members rather than the usual 15) produced a consensus report in the summer of 2015. In addition to its existing mandate on norms of responsible state behaviour and confidence-building measures, the GGE was mandated to consider 'the issues of the use of ICTs in conflicts and how inter-

29 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010), 8, http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

30 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), 7, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

national law applies to the use of ICTs by States'.[31] The GGE report succeeded in further developing norms and rules for state cyber conduct, suggesting for example that states refrain from ICT activity 'that intentionally damages critical infrastructure'.[32] The report recommends that a further GGE be created in 2016, although mere continuation of GGE studies may begin to suffer from diminishing returns. It is evident in the cyber security field that as countries move beyond statements of lofty general principles and begin to address specific measures, divisions of views become more pronounced and concrete outcomes more elusive. Ultimately, states will need to move beyond the restricted participation of the GGEs and embrace some form of broader, multilateral negotiating forum if the ideas being generated by the GGEs are to be transformed into agreed commitments.

7. Prospects for Cooperation

Despite the challenges that international cooperation on outer space and especially in the new domain of cyber security faces, there is also a growing parallel concern that the preservation of the peaceful environments of outer space and cyberspace are too important a set of objectives to leave only in the hands of the military. In both the case of outer space and cyberspace, and especially with the latter, there is a large and potentially influential civilian lobby comprised of business and civil society actors that is increasingly aware of the threats to cyberspace and is engaged in prodding governments into some preventive action. The private sector's refrain is that the time has come to establish a public-private partnership to address global cyber security threats and to develop policy responses, including the formulation of cyber security norms. As one large multinational firm has stated:

> 'The development of cybersecurity norms cannot be a niche foreign policy issue reserved for diplomats. Cybersecurity norms are an imperative for all users, governments, the private sector, non-governmental organizations, and individuals, in an Internet-dependent world – each contributes to the peace, security and sustained innovation of a globally interconnected society.'[33]

This civil society concern over the harmful consequences of a lawless cyberspace is starting to be manifested in diplomatic forums. At the UN General Assembly's fall

31 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 (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.

32 United Nations, General Assembly, *Group of Governmental Experts*, A/70/174, 8.

33 Microsoft Corporation, *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*, White Paper (23 January 2015), 14, http://www.microsoft.com/en-us/download/details.aspx?id=45031.

session in 2014, nine NGOs delivered a joint statement seeking action by states to adopt 'an effective international legal framework that will prevent cyber attacks and protect the networked infrastructure upon which societies rely for their wellbeing'.[34]

Barring another dramatic external event that draws attention to the vulnerability of these operating environments to disruption through irresponsible state behaviour, it may in fact be this private sector and civil society lobbying which will spur governments to take more decisive action. Although the work on outer space security pre-dates that on cyber security, it may well be in the latter realm that the first international security arrangements are devised. State authorities may feel a priority need to put down some initial markers of restraint regarding their conduct in cyberspace and to reassure the civilian sector that the government will not endanger this critical infrastructure through irresponsible action. The articulation of norms for responsible state behaviour, especially in the form of voluntary, political undertakings are likely to be the preferred route for states given their inherent flexibility and timeliness and the avoidance of the need to develop verification provisions that would have to underpin new international legal instruments.

Given the intrinsically global character of both outer space and cyberspace, it is understandable why much of the diplomatic consideration of the problem of security in these realms has occurred within the universal, multilateral context of the UN. Important complementary work has also been underway at the regional level, especially concerning cyber security. In Europe the Organization for Security and Co-operation in Europe (OSCE) has been active on the international security dimension of cyberspace and in April 2012 set itself the goal of developing a first set of CBMs 'to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs'.[35] The OSCE initiative yielded an initial set of CBMs that were approved at the organisation's December 2013 Ministerial meeting. Although the eleven measures adopted are primarily voluntary exchanges of information on various aspects of ICTs, there is provision for on-going institutional support by means of a dedicated working group that is to meet at least three times a year to discuss the information exchange and explore further CBM development.[36] The deterioration of East-West relations attendant upon the Ukraine crisis has likely put a damper on some of the cooperation envisaged by the CBMs, but the OSCE action stands out as the first multilateral agreement on cyber security CBMs and will probably serve as a model for others.

34 Women's International League for Peace and Freedom, *Civil Society Statement to First Committee on Cyber, Disarmament, and Human Security* (28 October 2014), http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com14/statements/28Oct_cyber.pdf.

35 Organization for Security and Co-operation in Europe, Permanent Council decision No. 1039, *Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1039 (26 April 2012), http://www.osce.org/pc/90169?download=true.

36 Organization for Security and Co-operation in Europe, Permanent Council 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.

Whether it occurs at the universal or regional level, the initiation of bilateral and multilateral consultations on how to ensure the continued peaceful exploitation of both outer space and cyberspace would usefully contribute to increased awareness, confidence-building and eventually the development of cooperative security arrangements. Given the potential mass disruption stemming from offensive cyber operations or space negation actions there should be an inherent interest on the part of states to engage in preventive diplomacy in these two realms. The intrinsically universal character of these two 'global commons' militates in favour of as inclusive a regime as possible and this in turn puts a premium on developing measures that can be agreed under UN auspices. It will be crucial for all concerned stakeholders to be pro-active in this regard and to begin to move now to preclude the most damaging manifestations of conflict in these vulnerable environments and thereby help sustain safe and secure access to them for all people at all times.

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

CHAPTER 9

International Legal Norms in Cyberspace: Evolution of China's National Security Motivations

Greg Austin

China, like most states, has sought to ensure that its interests are protected both by existing international law and in any discussion of emerging international legal norms. This chapter addresses China's pursuit of that goal in respect of its national security interests in cyberspace.[1] There is a brief overview of four essential background issues: the political character of norm diplomacy by any state, the security interests China has in cyberspace, the epistemic community in China involved in norm diplomacy, and the evolution of China's military cyber policy. The chapter then outlines three phases in cyber norm diplomacy by China: slow start (1998-2005), higher tempo where cyber war is more central (2006-2013), and the upgrade to a 'cyber power' ambition (2014 and beyond). The chapter ends with a short conclusion.

1. Legal Norms in Practical Diplomacy for Cyberspace

Diplomacy is in part a contest over the right to dictate international legal norms, how to have the upper hand in shaping them, or how to interpret and implement existing norms. Table 1 sets out this author's assumptions about the politicised terrain of norm formation in general and in respect of cyberspace in particular.

1 The author would like to acknowledge the useful comments by Professor Shen Yi of Fudan University, Jamie Collier of Oxford University and several anonymous reviewers.

An international legal norm can be one that is universally agreed (and therefore of universal application), or one limited to a group of consenting states (applying only to them). This distinction can be seen in the approach of the United States to the United Nations Convention on the Law of the Sea, which has near universal force in its entirety (subject to reservations lawfully registered and where permissible) but which the US honours only in so far as it reflects (in the US view) customary international law.[2] Universality of a norm, including implementation of all parts of it in its entirety, is not a prerequisite for it to be regarded as an international legal norm.

Under international law, each state is equal to all others in its right to offer interpretations of the meaning of its normative obligations. It must however rely on the court of international public opinion to win such claims. Therefore, China is as much a subject of norms and norm formation (along with almost 200 other states) as it is a state seeking to shape norms. China is obliged to be a norm-taker (analogy with 'price taker' in economics)[3] to a large degree, even as it aspires to be a norm-maker.

There should be no presumption of any kind regarding the potential universal appeal or moral rectitude of a normative proposition advanced by one state or another. A legal norm is the result of diplomatic compromise among the states which crafted it. Moral rectitude is in the eye of the beholder. Thus any privileging of one country's normative position over that of another state – for example suggesting that the US position is preferred over China's – is a statement of an individual ethical choice not one of political or legal analysis. The ethical terrain of cyberspace carries important dilemmas for states of all political stripes yet the need for new normative behaviours is urgent, as many of them have argued,[4] with considerable support from scholars.[5]

2 There are many iterations of this principle by the US. See for example, Office of the General Counsel of the National Oceanic and Atmospheric Administration, 'Law of the Sea Convention,' http://www.gc.noaa.gov/gcil_los.html: 'Although not yet a party to the treaty, the US nevertheless observes the UN LOSC as reflective of customary international law and practice'; see also Hillary Rodham Clinton, US Department of State, *Testimony before the Senate Committee on Foreign Relations* (Washington DC: 2012), http://www.state.gov/secretary/20092013clinton/rm/2012/05/190685.htm: 'As a non-party to the convention, we rely – we have to rely – on what is called customary international law as a legal basis for invoking and enforcing these norms'.

3 See for example Paul Krugman and Robin Wells, *Economics*, third edition (New York: Palgrave Macmillan, 2012), 16, https://books.google.com.au/books?id=_2YdBQAAQBAJ: 'A producer is a price taker when its actions cannot affect the market price of the good or services it sells'.

4 The best locations for government statements and analyses include UN documents, documentation on various conferences in the London Process accessible through the website of the 2015 conference in The Hague (GCCS2015, https://www.gccs2015.com/), and the INCYDER database of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (NATO Cooperative Cyber Defence Centre of Excellence, 'INCYDER,' https://ccdcoe.org/incyder.html).

5 Michael Portnoy and Seymour Goodman, eds., *Global Initiatives to Secure Cyberspace: An Emerging Landscape*, Vol. 42 (New York: Springer US, 2009); Markus Maybaum, Anna-Maria Osula and Lauri Lindström, eds., *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (Tallinn: NATO CCD COE Publications, 2015); Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Michael N. Schmitt and Liis Vihul, 'The Nature of International Law Cyber Norms,' *The Tallinn Papers* 5 (2014), Special Expanded Issue; Roger Hurwitz, 'The Play of States: Norms and Security in Cyberspace,' *American Foreign Policy Interests* 36 (2014): 322-331; Ludovica Glorioso and Anna-Maria Osula, eds., *1st Workshop on Ethics of Cyber Conflict: Proceedings* (Tallinn: NATO CCD COE Publications, 2014); American Bar Association, 'A Call to Cyber Norms: Discussions at the Harvard-MIT-University of Toronto Cyber Norms Workshops, 2011 and 2012' (2015), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2015apr14_acalltocybernorms.authcheckdam.pdf; 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); 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); Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas, *Baseline Review: ICT-Related Processes & Events: Implications for International and Regional Security (2011-2013)* (Geneva: ICT4Peace, 2014); Abdul Paliwala, 'Netizenship, Security and Freedom,' *International Review of Law, Computers and Technology* 27 (2013): 104-123.

Table 1. Indicative list of assumptions about the normative terrain of cyberspace.

Assumptions about the terrain of norms in international law
1. Politics, like diplomacy, is a contest over the right to dictate norms or at least have the upper hand in shaping norm development OR shaping an argument about how to interpret and implement existing norms.
2. An international legal norm can be one that is universally agreed (with universal application) or one limited to a group of consenting states (applying only to the consenting states).
3. Most new international legal norms with universal application usually take decades to develop and become accepted as norms.
4. Norms are often constituted by 'regimes' (of practice) that subsequently become legal norms.
5. Normative behaviours (such as consultation, self-restraint and dispute resolution by peaceful means) can be adjuncts to or even substitutes for legal norms.
6. Practices unregulated by norms coexist with emerging norms, universally accepted norms, and contested norms.
7. Discussions are often confounded by loose usage of the term 'norms' which has several meanings depending on the context (international legal norms, domestic legal norms, moral norms, political norms, professional norms, business norms, and so on).
Additional assumptions about cyberspace norms
1. Cyberspace is ubiquitous and highly variegated: the contest over norms, laws and practices of cyberspace is ubiquitous and highly variegated.
2. Some examples of the wide scope of cyberspace norms can be found in many areas of international law that directly touch on cyberspace issues, including intellectual property law, trade law, investment law, labour law, human rights, state responsibility, diplomatic (sovereign) immunity, law of the sea (cable protection), air and space law (satellite protection), air traffic control, disaster relief, pandemic control, laws of armed conflict, private international law, extradition treaties, and non-aggression treaties.
3. Ethical and political contest between states over the meaning of existing or emerging norms is severely magnified and exaggerated at all levels by the power of citizens accessing the internet and of private corporations who choose to mount active opposition to state preferences.
4. States are only one category of actor in cyberspace and they cannot exercise a monopoly position on shaping legal norms (power and authority are distributed away from states).

2. China Security Interests for Norms in Cyberspace

China has participated constructively in most international regimes governing cyberspace and observed most existing international law (legal norms), while contesting aspects of others, or pushing for new regimes and new norms. On the whole, it has maintained a positive record, with the main exception being its approach to human rights norms and a lesser exception being its approach to norms on protection of intellectual property rights affected by cyber espionage. China has been a participant in what Benson described as the 'spontaneous evolution of cyber law'.[6] In looking at the full scope of the regime complex underpinning the evolution of norms for cyberspace,[7] it is clear that China has been active in most of the forums identified by Joe

6 Bruce L. Benson, 'The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement without the State,' *Journal of Law, Economics and Policy* 269 (2005): 265.

7 Joseph S. Nye Jr, *The Regime Complex for Managing Global Cyber Activities* (Harvard: Belfer Center for Science and International Affairs, 2014), 7, http://belfercenter.hks.harvard.edu/files/global-cyber-final-web.pdf.

Nye. In this, it has often been a cooperative contributor to evolution of certain types of international legal norms, though these have usually been those less politicised and more related to business, the economy, trade, investment and technical standards. One indication of China's intent and exemplary record and attention to detail in these broader areas of economic security can be seen in the fact that a Chinese national, Zhao Houlin, secured international support in 2014 to head the International Telecommunications Union, having served as its Deputy Director General for seven years. Under his chairmanship, the conversations in the World Conference on International Telecommunications in 2015 were markedly different from the confrontational theatrics of the 2012 meeting, a fact that secured praise from the US.[8]

Looking at China's security interests in international aspects of cyberspace somewhat more narrowly, we can see that they are substantial and some cut across issues of the economy, business and technology transfer. They include:

- Preventing foreign interference in China's political sovereignty over Taiwan and Tibet;
- Constraining foreign actors from undermining the rule of the Communist Party;
- Preventing armed conflict;
- Constraining the military capability of its potential enemies;
- Maximising the country's military potential;
- Contingency planning for armed conflict;
- Intelligence collection and assessment;
- Protecting state secrets;
- Development of its defence industry base;
- Development of its national skills base for its military personnel;
- The protection of national critical information infrastructure (CII); and
- Mobilisation of the national economy and society in war-time if needed.[9]

Official Chinese views on these security needs in cyberspace are not usually documented in one place in such a comprehensive fashion but can be found in a variety of documents such as government defence white papers published every two years, especially the 2015 paper,[10] and the 2010 White Paper on the Internet in China.[11]

8 See Greg Austin, 'US-China Internet Cooperation,' *The Diplomat*, January 19, 2015, http://thediplomat.com/2015/01/us-china-internet-cooperation/.

9 These national security needs are not unique to China. For more detail on what they mean in the case of China, see Greg Austin, *Cyber Policy in China*, 1st edn (Cambridge UK: Polity Press, 2014), chapter 5; Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press, 2015); Daniel Ventre, 'Cybersécurité et cyberdéfense chinoise: évolutions', in 'Réflexions sur le cyber: quels enjeux?', ed. Jean-Christophe Pitard, *Bouet Centre d'études stratégiques aérospatiales* (2015): 128-142.

10 Ministry of National Defense the People's Republic of China, The State Council Information Office of the People's Republic of China, *China's Military Strategy* (May 2015), http://eng.mod.gov.cn/Database/WhitePapers/.

11 The State Council Information Office of the People's Republic of China, *The Internet in China* (June 8, 2010), http://www.china.org.cn/government/whitepaper/node_7093508.htm.

China, like many states, has not articulated in consistent detail how all of its individual security interests may be served by advocacy of this or that norm in cyberspace. This has left open the opportunity for speculation by analysts.

Security analysts in both the West and in China have often seen its position as focused largely on the fourth point in the list above: the need to constrain the cyber military capability of its potential adversaries. This has indeed been a high interest. Such a preoccupation would explain why China has focused some of its activities within the framework of the arms control mechanisms of the United Nations, especially the First Committee of the General Assembly. But China's interest in framing limitation of cyber weapons as a broad objective does not appear to have been followed up by its officials in any detail at the inter-governmental level.[12] It has subsumed this goal in pushing for reflection on and constraint of impulses toward militarisation of cyberspace, even though it very clearly joined the same trend in February 2014 when President Xi Jinping declared that the government would do everything necessary for China to become a 'cyber power'.[13]

That goal of constraining US cyber military power had in fact been just one of many national security priorities for China in its norm entrepreneurship for cyberspace. A wider view of its goals in cyberspace is both possible and necessary, not just within the international security domain but also outside it. First, China's national security interests are quite diverse and span a vast territory of policy interests. It is almost impossible to disaggregate any single one of them from others as a security motivator for China's position on cyberspace legal norms. Second, China has pursued cyberspace norm development for its national security interests hand in glove with its approach in areas affecting the economy, trade and development. The two domains of policy (national security and economic prosperity) are inextricably linked in China's conceptions of contemporary world order. China sees itself as needing a baseline of normative behaviour on cyberspace issues in order to maximise its economic exchange with the US, Japan and the European Union that it sees as essential for building an advanced military industrial base. Third, conflict prevention (stopping the escalation of political disputes to military confrontation) is also a paramount objective for China's leaders. At the same time, China has not for decades seen armed conflict with major powers as imminent and in that context has not been averse to active cyber probing of other countries' defences and civil infrastructure. It has clearly judged such actions to be low risk and low cost, and not prohibited by international law.

A wider view of national security, extending beyond the narrowly governmental or narrowly military, is also dictated by the fact that in cyberspace affairs, there are few neat boundaries between governments and the private sector, or to put the same point

12 It has figured prominently in Track 2 discussions involving Chinese officials.

13 The significance of this announcement is discussed in Austin, *Cyber Policy in China*, and several media commentaries by the author, such as: Greg Austin, '2015 is the Year of Chinese Cyber Power,' *East Asia Forum*, July 31, 2015, http://www.eastasiaforum.org/2015/07/31/2015-is-the-year-of-chinese-cyber-power/; Greg Austin, 'China's Military Dream,' *The Straits Times*, May 29, 2015, http://www.straitstimes.com/news/opinion/more-opinion-stories/story/chinas-military-dream-20150529; Greg Austin, 'How China Plans to Become a World Class Cyber Power,' *The Diplomat*, April 30, 2015, http://thediplomat.com/2015/05/how-china-plans-to-become-a-world-class-cyber-power/.

differently, between the national security aspects and the economic security aspect of cyberspace.

I have found only a small number of independent scholarly works that address the subject of this chapter systematically or in much detail. These include a number of articles by Chinese specialists about their government's approach to legal norms for cyberspace,[14] and these are complemented by a number of reports of international working groups involving Chinese participants.[15]

In terms of analyses outside the country, a short 2014 review on 'China and International Law in Cyberspace' provides a snapshot assessment of the situation around the end of 2013.[16] It observed that China's approach to norms for cyberspace was different to those of the US, though the bulk of the article bears out the opposite conclusion – that there has been more common ground than division. It noted that China strongly advocated the application to cyberspace of the UN Charter norm of non-interference in the internal affairs of other states. The article also discussed the notion, supported by China, that democratisation of Internet governance, and therefore the elimination of the strong US influence over the Internet Corporation for Assigned Names and Numbers (ICANN), conformed to a normative principle of good order, a principle the US also accepts. The analysis concluded that China's agreement to the 2013 report by the UN Group of Governmental Experts (GGE) on cyberspace issues suggests that 'China agrees in principle not only to the general application of international law to cyberspace, but also the application of specific aspects of international law, including the law of state responsibility, concepts in the UN Convention relating to the use of military force, and the law of armed conflict'. This was also the US position. The paper concluded that the 2013 GGE report represented 'an implicit, general consensus on the definitions of key terms such as 'use of force' and 'armed attack' in cyberspace',[17] a view of the GGE report that is not really credible. A 2014 legal analysis from the US, 'An International Law Response to Cyber Economic Espionage', provides a useful analysis of the place of existing norms and organisations such as the WTO to address charges levied at China.[18] By implication, it suggests correctly that China is already party to norms governing this practice. Michael Swaine provides a useful overview of how China views its interests in cyberspace and its general approach to norm development.[19]

14 See for example, Zhang Xinbao, 'Establishing Common International Rules to Strengthen the Cooperation of Cyber Information Security,' *China Legal Sciences* 121 (2013) [in Chinese]; Shen Yi, 'Protecting Safety by Strength or Achieving Safety by Governance? – Two Cyber Safety Strategies and China's Choice,' *Foreign Affairs Review* (2013): 140-148 [in Chinese]; Chunmei Kang, 'Establishing Norms of Behaviour in Cyberspace: The Chinese Viewpoint,' in *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*, Revised edition, ed. Giampiero Giacomello (London: Bloomsbury Publishing, 2014), 113-124.

15 Center for Strategic and International Studies (CSIS), *Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR)* (June 2012), http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf; and Karl Frederick Rauscher and Zhou Yonglin, 'Frank Communication & Sensible Cooperation to Stem Harmful Hacking,' *EastWest Institute* (2013). A full version can be found on the website of CERT China at http://www.cert.org.cn/publish/main/upload/File/China-US%20Anti-Hacking%20Report%20v190.pdf.

16 Kimberly Hsu and Craig Murray, *China and International Law in Cyber Space, U.S.-China Economic and Security Review Commission Staff Report* (U.S.-China Economic and Security Review Commission, 2014), 1.

17 Ibid, 4.

18 Christine Parajon Skinner, 'An International Law Response to Cyber Economic Espionage,' *Connecticut Law Review* 46 (2014): 1165-1207.

19 Michael D. Swaine, 'China's Views of Cyber Security in Foreign Relations,' *China Leadership Monitor* 42 (2013), http://carnegieendowment.org/files/clm42ms_092013carnegie.pdf.

Since this chapter is about 'China the government', it focuses on official views. A government's view of international legal norms is only what it says it is or, in some cases, what it may unambiguously manifest by its actions over a sustained period. China's official views on international legal norms for cyberspace can be found in UN resolutions that China has supported beginning in 1998, in statements by Chinese officials in the UN General Assembly and its committees, in the World Summit on the Information Society (WSIS), the International Telecommunications Union (ITU), the UN-initiated Group of Governmental Experts (GGE) over several iterations,[20] regional organisations, and in several treaties with a cyberspace aspect, such as the 2009 Treaty among members of the Shanghai Cooperation Organization (SCO),[21] the Beijing Convention 2010[22] on aircraft hijacking (with a clause on technical attack), and the Russia/China information security agreement of 2015.[23] China's views can also be found in consideration of treaties it has rejected, such as the 2001 Budapest Convention on Cyber Crime and the 2012 Multinational Statement on Nuclear Information Security agreed by 31 states at the Nuclear Safety Summit that year. At the same time, unofficial analytical sources or working group reports do reflect opinions of senior government leaders and can be valuable supplementary material if carefully scrutinised.

20 The work of the Group of Governmental Experts set up by the United Nations to review certain aspects of international law relating to cyberspace provided the Chinese representatives the opportunity to outline Chinese official positions at far greater length and to sound out alternative approaches. Unfortunately, there is no public record of the Chinese representative's positions in these meetings, and only a few passing references from other participants to the positions they believe the Chinese representatives took. The formal reports of the GGE are mentioned later in terms of how they illuminate China's public position.

21 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]. The text in Russian of the treaty, with unofficial English translation, can be found at NATO Cooperative Cyber Defence Centre of Excellence, 'Shanghai Cooperation Organisation,' https://ccdcoe.org/sco.html.

22 The text of the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation 'was adopted with 55 votes in favour, 14 votes not in favour' and the text of the 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft was adopted 'with 57 votes in favour, 13 votes not in favour'. See International Civil Aviation Organization, *Final Act of the of the International Conference on Air Law (Diplomatic Conference on Aviation Security) held under the auspices of the International Civil Aviation Organization at Beijing from 30 August to 10 September 2010* (10 September 2010), http://www.icao.int/secretariat/legal/Docs/beijing_final_act_multi.pdf. For the text of the Convention, see *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, Beijing, 10 September 2010, No. 21, https://www.unodc.org/tldb/en/2010_convention_civil_aviation.html. For the text of the Protocol, see *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*, Beijing, 10 September 2010, No. 22, https://www.unodc.org/tldb/en/2010_protocol_convention_unlawful_seizure_aircraft.html. For an excellent analysis of the two treaties, see Damien van der Toorn, 'September 11 Inspired Aviation Counter-Terrorism Convention and Protocol Adopted,' *American Society of International Law* 15 (2011), http://www.asil.org/insights/volume/15/issue/3/september-11-inspired-aviation-counter-terrorism-convention-and-protocol. According to the International Civil Aviation Organization (ICAO), the main changes to pre-existing treaties with similar names were the criminalisation of the acts of using civil aircraft as weapons, using dangerous materials to attack aircraft or other targets, and cyber attacks on aircraft in flight.

23 For a text in Russian, see Government of the Russian Federation, Order of the Russian Government on signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of Ensuring International Information Security, 30 April 2015, 788-r, http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [in Russian].

3. China's Epistemic and Policy Communities

The characteristics of a country's epistemic and policy communities will shape how it analyses and proposes norms and normative ideas on the international stage. Much will depend on the values and the discourse about values in domestic politics. In cyberspace affairs, there is a fundamental gulf in domestic approaches to the articulation of international legal norms between, on the one hand, China and like-minded countries such as Russia and, on the other, the US, the European Union, Japan and other Western countries. This chapter is not the place to analyse differences between epistemic communities or its impact on the subject at hand.[24] Let it suffice for current purposes merely to observe that a dialogue with China on norms about cyberspace affairs may be challenging because of differences between the structure and priorities of the epistemic and policy communities inside China compared to those in major Western powers. After all, as Nye has observed, norm development relies on epistemic communities.[25] If the epistemic communities are very different, then we must expect differences between national approaches to norm promotion.

We can cite, as just one example, the fact China has not been as vigorous as its Western counterparts in forensic dissection of existing international legal norms about the permissibility or otherwise of certain actions in cyberspace in time of war or in preparation for war. China has shown little interest even in a scholarly elaboration of possible approaches to cyber norms, such as the Tallinn manual.[26] A far higher priority has been the articulation of cyberspace norms affecting political sovereignty at home in terms of controlling dissent and maintaining Communist Party rule. Simply put, the Government of China has a very basic view on national security aspects of international legal norms for cyberspace and they relate mainly to internal security.

In the absence of legal doctrines on the military uses of cyberspace that might emanate from the Ministry of Foreign Affairs or the Ministry of National Defence, we are left to speculate as to official views on key issues.

We can assume that it is China's view, as it is that of most countries, that all activities preparatory for military combat (and national self-defence) not specifically prohibited by international law are permissible. This is captured well, between the lines, in the text of the 2015 agreement with Russia that commits each country to refrain from 'unlawful' interference in the information infrastructure of the other. This assessment is also captured directly in the language of a 2010 international treaty and associated protocol both signed by China and the US among others, that requires states to criminalise 'technological attack' (i.e. including cyber

24 An overview of China's values for cyberspace affairs can be found in Austin, *Cyber Policy on China*.
25 Joseph S. Nye Jr, 'The Information Revolution and American Soft Power,' *Asia-Pacific Review* 9 (2002): 60-76.
26 Schmitt, *Tallinn Manual*.

attack) against civil aviation. Article 6 of the Protocol excludes situations of armed conflict and the lawful duties of the armed forces of a state from the purview of the treaty and protocol.[27] Similar language can be found in other international treaties excluding their effect from situations of armed conflict and the lawful duties of the armed forces of a state.

Thus this chapter can throw some light on what China has hoped to get out of discussion on legal norms in terms of protecting or advancing its military security interests. But this will look and feel very different from the articulation of such expectations about norms among legal experts and political scientists in the West. The chapter is more useful for seeing how China sees the interaction in the international normative space between national security narrowly defined and broader conceptions of it based on economic interests.

4. Milestones in China's Cyber Military Policy

This section of the chapter gives a very brief summary of how China's military interests in cyberspace have developed from 1998 to the present. The purpose is not to tie subsequent discussion too narrowly to military affairs, but rather to reinforce the proposition that military use of cyberspace is a relatively new area of policy for China (beginning around 2003) and one that has developed only in fits and starts before taking a decisive turn in 2014.

China, like all states, has had to come to terms with a revolution in military affairs as a result of the rapid advance in the military potential of information and communications technologies. In 1998, the US published a formal Joint Staff doctrine on Information Operations (to include offensive computer attack),[28] that had been many years in the making and which brought together elements that had been well practised in the single military services and separate intelligence agencies of the US. The same year, two Chinese military strategists were writing a book called *Unrestricted Warfare*, expressing concern about a range of developments, including information warfare, and foreshadowing an eventual shift by China to a similar strategy that US had adopted.[29] Yet China was behind at the time. Table 2 offers a brief summary overview of milestones in China's military policy in cyberspace.[30]

27 These treaties are analysed in Greg Austin, Eric Cappon, Bruce McConnell and Nadia Kostyuk, 'A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets,' *EastWest Institute* (2014): 17-18.

28 United States of America, Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (9 October 1998), http://www.c4i.org/jp3_13.pdf. This doctrine manual, which included options for computer network attack, was developed to implement a DoD Directive on Information Operations from 1996, the first of its kind in the US at joint force level.

29 See Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999) [in Chinese], http://www.c4i.org/unrestricted.pdf. The book was written through 1998. A translation more than 200pp of excerpts is available at http://www.c4i.org/unrestricted.pdf. The book is notable for its several references to the breach of international norms or rules by any countries adhering to the concept of 'unrestricted warfare'.

30 For a discussion of the detail, see Austin, *Cyber Policy in China*, chapter Five.

Table 2. Milestones in China's military development in cyberspace.

1998	Chinese military pays closer attention to military uses of cyberspace
1999	China observes US cyber operations against Belgrade electric grid
2000	Jiang Zemin declares shift to an information society, including in military affairs, and asks PLA to begin to shift focus
2001	PLA joins Informatisation Leading Group which is upgraded from Vice Premier control to Premier
2003	China shifts official military doctrine to take account of informatisation China conducts first mass cyber espionage 'Titan Rain'
2006	Training regulations for information warfare approved National Informatisation Plan 2006-2015 (first such plan in in the civil economy)
2007	China undertakes a kinetic anti-satellite test (US cyber military power depends on space-based assets)
2010	Internet white paper says China's cyber military capabilities are rudimentary
2011	Changes in General Staff communications structure Academy of Sciences publishes 2050 Roadmap for Information Technology
2013	Edward Snowden revelations deliver a sharp wake-up call to China's leaders and security elites
2014	Xi declares China will become a 'cyber power' and takes over Leading Group; six months later Xi calls for a cyber military strategy
2015	China issues first 'Military Strategy' recognising outer space and cyberspace as the 'commanding heights' of international security

A simple time-line like this cannot convey the complexity of the military policy changes contemplated by China in the past 15 years, the immense bureaucratic and practical obstacles China would face in implementing any policy change, or the character of its international relations over the protracted time frame the changes would need to be made.

One essential conclusion to draw from this timeline is that China's approach to international legal norms for cyberspace would have trailed behind this timetable, and not got ahead of it. If the pace of adjustment in cyber military affairs was gradual, then so too would have been the pace of development of an approach to international legal norms governing military affairs. Moreover, since the most radical changes in cyber military policy only occurred in 2014 and 2015, we can probably expect to see some acceleration in the pace around development of approaches to international legal norms for security in cyberspace. The situation with respect to internal security was markedly different, with China staking its positions in that area quite early by comparison.

5. Slow Start: 1998-2005

National security concerns only began to surface in China's international legal practice for cyberspace around 1998 when it supported a resolution introduced by Russia in the First Committee on security aspects of information and telecom-

munications.[31] The Resolution (less than two pages long) seemed unremarkable. It cited three normative propositions: optimum exploitation of information and communications technologies (ICT) for development through broad international cooperation; fostering strategic stability and state security; and the need to prevent criminal or terrorist use of the technologies. Key elements of the original Russian draft had been dropped at the urging of the US. These deletions involved references to the use of information technology for military purposes, specific definitions of 'information weapons' and 'information war', the need for a regime of prohibition of the creation and use of information weapons, and provisions on the comparability of the impact of information weapons and weapons of mass destruction.[32] In the same UNGA session, China supported a resolution (passed without a vote) which contained a section on 'Information in the Service of Humanity' in which it called for freedom of the press, a diverse media and rapid transfer to developing countries of information technologies.[33] This resolution had carried over from previous years. Thus, in 1998, China was not really thinking in terms of crafting new international legal norms to govern cyberspace and there was wide agreement on the need to foster strategic stability and state security (expressed in the most general terms).

Throughout 1998 and 1999 China got a foretaste of the potential of international cooperation on cyberspace security issues when it found itself working alongside the rest of the world to prevent any dangers from the Y2K problem.[34] At this time, Russia's relations, under Boris Yeltsin, with the US were quite strong. Russia had just been admitted to the G8, and the two Presidents had agreed to include cyber security in their official bilateral agenda.[35] Yet the divergence in approaches in the international community that the Russian-sponsored 1998 Resolution (53/70) was to open up were more fully revealed in a 1999 report by the UN Secretary General recording the formal position of ten member states provided by them in accordance with the terms of the Resolution.[36] In its statement, Russia called for work to 'begin on the development of international principles (e.g. a regime, a code of conduct for states)' to strengthen international information security, with such principles subsequently 'incorporated into a multilateral international legal instrument', and working in partnership with the UN Conference on Disarmament.[37] In its response,

31 United Nations, General Assembly resolution 53/70, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/53/70 (4 January 1999), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70.

32 Aleksandr Berditskii, 'An International Agreement on Cyber Security: Is Consensus Possible?' *Perspektivy*, October 24, 2014, http://www.perspektivy.info/table/mezhdunarodnyje_dogovoronnosti_po_kiberprostranstvu_vozmozhen_li_konsensus_2013-10-24.htm [in Russian].

33 United Nations, General Assembly resolution 53/59, *Questions relating to information*, A/RES/53/59 (18 February 1999), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/53/59. Section A in this resolution related to 'information in the service of humanity'.

34 This was the concern that when the century and millennium rolled over at midnight on 31 December 1999, then many automated controllers in sensitive systems (such as aircraft, nuclear power stations, financial institutions or hospitals) might malfunction since programmers may not have provided for a '00' or '000' date after '99' or '999'.

35 See Franz-Stefan Gady and Greg Austin, 'Russia, the United States and Cyber Diplomacy: Opening the Doors,' *East West Institute* (2010): 1-2.

36 United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General,* A/54/213 (10 August 1999).

37 Ibid, 9.

the US was silent on emerging doctrines of information warfare, and declared that 'it would be premature to formulate overarching principles pertaining to information security in all its aspects'.[38] The US and its allies had a clear preference to keep cyberspace issues at the United Nations out of the purview of the First Committee (disarmament) where the Russians had introduced it. China was silent on this emerging debate about a new treaty held up by Russia in 1999.

Thus in 1999, the US position was identical with the position of China in 2015 outlined later: that it may be premature to formulate over-arching principles, especially in regard to cyber warfare.

Subsequent versions of the annual resolution became more strident on security issues of concern to China and Russia. In the 1999 NATO war against the former Yugoslavia, the potential of information warfare was played out in several ways on which the public historical record is incomplete.[39] Regardless of what actually transpired, there was some currency to the idea that network attack weapons had been used by the US for the first time ever in war. President Jiang Zemin was prepared to credit the reports as fact[40] and his mind had been focused no doubt by what China saw as a precision (kinetic) attack by NATO on the Chinese Embassy in Belgrade. The 2000 version of the UN ICT/security resolution for the first time called on states to promote 'possible measures to limit the [security] threats emerging in this field'.[41] Thus the idea was born that China and Russia wanted to use an arms control process of some sort to constrain US and allied capability, even though the US also supported this new language.

In 2000, Jiang Zemin appealed in a brief reference during a speech in Beijing to the World Computer Congress for a global Internet treaty in order to jointly strengthen information security management and to give full play to the 'positive role of the internet'.[42] His interventions coincided with the emergence in the G8 of the Okinawa Declaration on a Global Information Society[43] which sought to promote a globally inclusive approach, but which remained largely a G8 exercise, including through its Digital Opportunity Task Force. At this time, China did not have a fully articulated diplomatic strategy for international security aspects of the information society, beyond those that affected economic settings, science

38 Ibid, 13.

39 For one account, see Myriam Dunn Cavelty, 'Cyberwar' in *The Ashgate Research Companion to Modern Warfare*, eds. George Kassimeris and John D. Buckley (England: Ashgate Publishing Limited, 2010), 123-144.

40 See Jiang Zemin, 'Informationize the Army, Excerpts form a speech to the Central Military Commission, 27 December 2002,' in *On the Development of China's Information Technology Industry*, ed. Jiang Zemin (Oxford: Elsevier, 2010) (Oxford: 2010), Kindle edition. Jiang cited NATO's rout of the Yugoslav army as an example of informatised, non-contact warfare.

41 United Nations, General Assembly resolution 55/28, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/55/28 (20 November 2000), Article 1, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/28. In the 1998 resolution, this language did not appear. In the 1999 resolution, it appeared only in a preambular reference.

42 Jiang Zemin, 'Speech at the Opening Ceremony of the 16th World Computer Congress', in *On the Development of China's Information Technology Industry*, ed. Jiang.

43 See Ministry of Foreign Affairs of Japan, *Okinawa Charter on Global Information Society* (2000), http://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html.

and technology or domestic security, including cyber crime.[44] Nevertheless, it was actively trying to position itself in the diplomatic space especially with reference to a possible new treaty, Internet governance and ICANN.[45] In 2000, a Chinese candidate for a seat on the Council of ICANN was unsuccessful but a researcher from the Chinese Academy of Sciences was elected as Council Chairman of Asia Pacific Top Level Domain Association (APTLD) by a unanimous vote. For China, ICANN arrangements have related directly to international security order because of the presumption that if governments like the US and like-minded countries controlled the governance of the Internet, they would continue to stimulate the flow of subversive material over it against the interests of states like China.[46]

China took a more robust and engaged position on international collaboration on cyberspace issues in the framework of the Asia Pacific Economic Cooperation (APEC) group in support of its international economic security interests, including protection of critical infrastructure. One factor that facilitated China's willingness to extend itself in APEC on debate about cyber-related norms or normative behaviour was that this group was fairly tightly focused on economic issues, studiously avoiding politically contentious issues (to the extent that China had ten years earlier agreed to Taiwan's membership as an 'economy'). This consideration meant that China did not have the same need or the potential in APEC to deal with political and security issues as it did in the UN framework. In October 2001, in the month after the 9/11 attacks in the US, China joined the APEC leaders in a statement after their summit in Shanghai that called for strengthening cooperation at all levels in counter-terrorism, including the protection of critical infrastructure, such as telecommunications.[47] The leaders also issued a lengthy action plan on developing *e*-APEC, which included many commitments by China to normative behaviour in the economic and social spheres of cyberspace development, including security, privacy protection, and consumer trust.[48]

In May 2002, APEC Telecommunications Ministers, including China, agreed the Shanghai Declaration,[49] which included as Annex A the Work Programme for their officials,[50] and at Annex B, a more detailed 'Statement on the Security of Information and

44 On 4 December 2000, China supported a UN General Assembly Resolution 'Combating the criminal misuse of information technologies'. See United Nations, General Assembly resolution 55/63, *Combating the criminal misuse of information technologies*, A/RES/55/63 (22 January 2001), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

45 ICANN was incorporated as non-profit, non-governmental organization in 1998, but remained formally associated with the US Department of Commerce until 2015.

46 See for an example of hundreds of commentaries to this effect over many years, Guo Ji, 'The Internet Cannot Be Allowed to Become a New Tool of US Hegemony,' *English Edition of Qiushi Journal* 6 (2014), http://english.qstheory.cn/magazine/201401/201401/t20140121_315162.htm. *Quishi* is a journal of the Chinese Communist Party.

47 Asia-Pacific Economic Cooperation, *APEC Leaders Statement on Counter Terrorism* (21 October 2011), http://www.apec.org/Meeting-Papers/Leaders-Declarations/2001/2001_aelm/statement_on_counter-terrorism.aspx.

48 Asia-Pacific Economic Cooperation, *APEC Economic Leaders Declaration Appendix 2: e-APEC Strategy*' (21 October 2001), http://www.apec.org/Meeting-Papers/Leaders-Declarations/2001/2001_aelm/appendix2_eAPEC_strategy.aspx.

49 Asia-Pacific Economic Cooperation, *The Fifth APEC Ministerial Meeting of the Telecommunications and Information Industry (TELMIN5), Shanghai Declaration*, TELMIN5/1 (29-30 May 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2002_tel/.

50 Asia-Pacific Economic Cooperation, *Annex A – Program of Action*, *Shanghai Declaration* (29-30 May 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2002_tel/annex_a.aspx.

Communications Infrastructures.[51] The annex expressed shared recognition of interdependence of the information infrastructure in cyberspace and, indeed, the interdependence of the information security of all members. The Programme of Action provided an impetus for convening expert groups on security related issues. As the APEC host, China has to be credited at least in part with the emergence of these processes.

These moves early in the decade were largely declaratory but provided a strong foundation for a leading role later by China in regional approaches and they closely foreshadowed the agreements on critical infrastructure supported by the Chinese representative in the 2013-2015 GGE convened by the United Nations.

At the Ministerial Meeting of APEC in Los Cabos, Mexico, on 23-24 October 2002, the participants agreed the 'importance of protecting the integrity of APEC's communications and information systems while allowing the free flow of information'.[52] They 'supported' the 'Cybersecurity Strategy' which had been presented by the APEC Telecommunications and Information Working Group (in fact drafted by the US), and they 'instructed Officials to implement the Strategy'. By this time, China had decided on a policy of social control of the Internet, realising that it could not ever achieve the technology to censor it completely.[53] At the same time, China continued to maximise its technical capacities, and build the foundations of the biggest and most intrusive cyber-enabled internal surveillance system in the world.[54]

In the United Nations setting, the 2002 version of the annual Russian-instigated ICT resolution saw a slight change in language. The preambular clause on the threats, previously very broad ('may affect the security of states'), now specifically called out a 'threat to the integrity of the infrastructure of states to the detriment of their security in both civil and military fields'.[55] At this time, China began to stake out its independent views (unilaterally expressed) on legal norms for cyberspace, flagging them for the first time in a rather general statement in 2002,[56] and reiterated in similar statements in 2004[57] and 2006.[58] China called for the use of

51 Asia-Pacific Economic Cooperation, *Annex B – Statement on the Security of Information and Communications Infrastructures, Shanghai Declaration* (29-30 May 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2002_tel/annex_b.aspx.

52 See Asia-Pacific Economic Cooperation, *2002 APEC Ministerial Meeting. Joint Statement - Expanding the Benefits of Cooperation for Economic Growth and Development - Implementing the Vision* (23-24 October 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Annual/2002/2002_amm.aspx.

53 See Austin, *Cyber Policy in China*, chapter 3.

54 Arguably, the US has the biggest and best capability for surveillance, but in terms of negative impact, relatively speaking, on the lives of people, it is China which has the more intrusive surveillance system.

55 General Assembly resolution 57/53, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/57/53, (30 December 2002), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/53.

56 'Statement by Ambassador Sha Zukang Head of the Chinese Delegation at the First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society' (The First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society, Geneva, 1 July 2002), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t25077.shtml.

57 See United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/59/116 (23 June 2004), 4, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/407/04/PDF/N0440704.pdf?OpenElement: 'China holds that use of information technology should abide by the United Nations Charter and other internationally accepted principles'.

58 United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/61/161 (18 July 2006), 4, https://disarmament-library.un.org/UNODA/Library.nsf/df4241a26771ddbd852571a8006cd413/8cc65546257a1692852571cb00566c6e/$FILE/sg61.161.pdf.

information technologies in accordance with the UN Charter, including in respect of international security. As indicated in Table 2 above, it was at precisely this time that China was preparing the ground for its first shift to information war strategies in response to what it had seen the US and Russia developing.[59]

In the 2002 statement, China's Ambassador to the United Nations in Geneva, Sha Zukang,[60] articulated the need for innovations in diplomacy to respond to the information society: 'establishing international organisations and mechanisms that ensure the security and reliability of communication networks by fighting against viruses and cyber crimes'.[61] China's engagement in the preparations for the World Summit on the Information Society became an additional opportunity (a workshop) for the development of its normative positions. Sha offered an assessment of the current global situation with respect to the information society. Alongside unprecedented technological conditions for global economic and social development, and valuable 'digital opportunities' for economic development and social progress, he observed that the 'infocom' development around the world is 'seriously unbalanced'. The digital divide is 'widening instead of narrowing, putting the developing countries in a more disadvantageous position'. He warned that this would 'inevitably further aggravate the social and economic disparity' and that the digital divide had to become a major focal point of international action.

His also laid out a six-point position statement on what states might do. First, he said, since 'countries vary in their social and cultural traditions and level of economic development and informatisation, plans and measures they formulate for their own informatisation may well differ'. Second, information infrastructure is the 'physical foundation of the information society' and in the future it needs to 'satisfy our demand for intelligence, diversification, personalisation, multimedia and globalisation as well as universal service'. Considerable attention needed to be given to developing countries to 'accelerate their information infrastructure build-out'.

The third point addressed security more directly. He noted that this was multi-level, from promoting consumer confidence to countering terrorism. He said that this involved technologies as well as laws and regulations and would require international cooperation. Fourth, to foster the expansion of knowledge and skills, innovative mechanisms for training and human resources development were needed. Fifth, developed countries needed to 'truly shoulder their responsibilities in helping the developing countries accelerate their informatisation processes'. Assistance could take the form of financial support, technology transfer and human resources training. Sixth, the private sector and the civil society would need to be closely involved but in international policy, 'governments obviously should play the leading role'.

Subsequently, China started to firm up its commitment to the goals of common security in an interdependent cyberspace. This can be seen in its support for the

59 See Austin, *Cyber Policy in China*, 132-35.

60 Sha subsequently became the Under-Secretary-General of the United Nations responsible for the Department of Economic and Social Affairs (UNDESA). He was succeeded by compatriot, Wu Hongbo.

61 Statement by Ambassador Sha Zukang.

December 2002 UN General Assembly Resolution (ARes/57/239) on 'Creation of a global culture of cybersecurity' and for the 2003 Geneva Declaration of Principles of the World Summit on the Information Society. This latter document observed that '[s]trengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs'.[62] The Association of South East Asian Nations (ASEAN) agreed with China in 2003 to implement an ASEAN-China Strategic Partnership for Peace and Prosperity, with a declaration that expressed their joint intent: 'to formulate cooperative and emergency response procedures for purposes of maintaining and enhancing cybersecurity, and preventing and combating cybercrime'.

The earlier UN resolutions beginning in 1998 had the effect of saying that information technologies were of concern to international and national security, whereas the other documents of 2002 and 2003 mentioned above saw China signing up to more explicit statements of what that meant and what should be done about it with other states. These themes as canvassed at the time were not much different in effect from what China's GGE representative agreed to in 2015.

In 2004, the United Nations convened its first GGE to consider security aspects of ICT. That year, in its first statement to the Secretary General in connection with the call that was made in the first ICT/security resolution in 1998 for states to register their views, China made a fairly strong if brief intervention.[63] It said that 'information security has become a grave challenge in the field of international security'. China declared its support for 'international efforts aimed at maintaining and promoting information security of all countries', and it also supported the establishment of governmental expert group to discuss how common understandings on the issues might be advanced at the international level. The statement called for special attention to 'information criminality and terrorism'. It reiterated the view that the 'imbalanced development of countries in the field of telecommunications' mandated a need for the international community to deepen cooperation in the research and application of information technology. In 2004, as part of a consultation mechanism for trilateral relations in the broad, which had been established at head of state level the year before, China, Japan and Korea agreed a work plan that included 'projects on network and information security policies and mechanisms, joint response to cyber attacks (including hacking and viruses), information exchange on online privacy protection information, and creation of a Working Group to promote this cooperation'.[64]

In 2005, China supported the Lima declaration by APEC Telecommunications

62 First Phase of the World Summit on the Information Society, *Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/4-E (12 December 2003), http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

63 United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/59/116 (2004).

64 Portnoy and Goodman, eds., *Global Initiatives to Secure* Cyberspace, 55.

Ministers[65] which mentions their recognition of the 'importance of ensuring the security and integrity of the APEC region's communications infrastructure, in particular the Internet, in order to bolster the trust and confidence of users and enable the continued advancement of this infrastructure'. Several other APEC policy documents, signed off by China, were adopted that year:

- Guiding Principles for PKI-Based Approaches to Electronic Authentication;
- Principles for Action against Spam; and
- Strategy to Ensure a Trusted, Secure and Sustainable Online Environment.

By August 2005, it had become apparent that the first GGE, which had been set up in 2004, would not reach 'consensus on a final report'.[66] According to the Russian representative, all members of the group (including China) but not the US representative, had agreed a number of points:

- The capability of ICT as an effective means of negatively affecting the civil and military affairs of a state;
- The powerful destructive force of information aggression;
- The potential for harmful acts in the information space both from states and non-state actors (criminals and terrorists);
- The existence of capabilities within states for covert use of cyber criminals; and
- The need for mutual efforts to reduce threats and strengthen trust in the information sphere.[67]

Thus, by 2005, China had moved decisively on normative approaches to economic security aspects of cyberspace on the diplomatic and international legal stages. In party with other states, it had called out counter-terrorism as a key security issue to be addressed through legal norms or normative behaviours in cyberspace and was calling out the need to be prepared for 'information aggression'. China's experience reviewed above shows that APEC and a number of regional mechanisms (such as Japan-China-Korea trilateral) were more productive than the UN as a forum on cyberspace norms.

65 Asia-Pacific Economic Cooperation, *2005 APEC Telecommunications and Information Ministerial Meeting, Lima Declaration* (1-3 June 2005), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel.aspx.

66 See United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/60/202 (5 August 2005), 2, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement.

67 Andrey Krutskikh, 'Towards a Politico-Legal Foundation for Global Information Security,' *International Trends*, http://www.intertrends.ru/thirteen/003.htm [in Russian].

6. Higher Tempo: Cyber War more Central 2006–2013

China took a dramatic step in 2006 through its membership of the Shanghai Cooperation Organization (SCO) when it supported a declaration by it on information security.[68] This manifestation of China's strategic intent in normative debates on cyberspace included an assessment of the revolutionary impact of ICT on security: 'ICTs are shaping the global information environment, on which foundation rests the political, economic, defence, socio-cultural and other components of national security and of the entire system of international security and stability'. The statement expressed concern about a 'real danger that ICT would be used for the purposes of bringing serious harm to the security of the individual, society and states by breaching fundamental principles of equality and mutual respect, non-interference in internal affairs of sovereign states, the peaceful settlement of disputes, non-use of force, and the observance of human rights'. The signatories called for a range of unspecified measures at bilateral, multilateral and global levels to address the new threats.

This declaration was referred to in the final communique of the summit as 'Statement of Heads of State of Member States of the Shanghai Cooperation Organisation on International Information Security'.[69] The communique declared that 'Threats of a military-political, criminal or terrorist nature to information security constitute common challenges for all member states that need to be dealt with through prompt joint measures'. It noted that an SCO experts' panel had been 'entrusted with the task of producing a long-term plan of action for the maintenance of information security before the next Summit in 2007, including ways of solving this problem within the SCO framework'. One import of this was that the membership of the SCO (all authoritarian states) strongly identified with China's positions on most issues, especially the balance to be struck between state sovereignty and international openness. According to a later Russian study, the Heads of State agreed that the threats to international information security should be dealt with through the observance of international law.[70] (This presaged China's support for the same proposition in the 2013 report of the UN GGE report discussed later.)

In a statement to the UN in 2006, China went much harder on the need for states to respect the differences in political systems, asserting that understanding of the principle that the free flow of information 'should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be

68 *Declaration of the Heads of Member States of the Shanghai Cooperation Organization on International Information Security* (15 June 2006), http://www.sectsco.org/RU123/show.asp?id=107 [in Russian].

69 'Joint Communiqué of the Meeting of the Council of Heads of State of the Shanghai Cooperation Organization' (The Council of Heads of State of the Shanghai Cooperation Organization, Shanghai, 15 June 2006), http://www.china.org.cn/english/features/meeting/171590.htm.

70 Berditskii, 'An International Agreement on Cyber Security: Is Consensus Possible?'

respected'.[71] It asserted its doctrine that there is a legally-bounded, sovereign cyberspace, a Chinese Internet: 'each country has the right to manage its own cyberspace in accordance with its domestic legislation'. It positively appraised the work of the GGE because it offered the opportunity for a 'profound exchange of ideas and offered numerous valuable proposals', even though it failed to produce a consensus report. It indicated its support for reconvening a similar group.

In 2006, the ASEAN Regional Forum (ARF), a cooperative security and preventive diplomacy forum for heads of states and/or foreign/defence ministers of the ASEAN states plus China, Russia, the US, Japan, North and South Korea and Australia, among others,[72] issued a statement on security in cyberspace, acknowledging the 'importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyberspace and encourage the formulation of such a framework'.[73] It recognised the 'serious ramifications of an attack via cyberspace to critical infrastructure on the security of the people and on the economic and physical well-being of countries in the region', as well as 'stressing the need for cooperation between governments and the private sector in identifying, preventing, and mitigating cyber-attacks'. The statement was largely focused on cyber crime and cyber terrorism, and it called on states to make necessary changes to domestic law enforcement as we cooperate internationally.

At the summit of SCO Heads of State in August 2007, the members signed a series of documents, among which was an 'SCO member countries' action plan to safeguard international information security'.[74] It committed them to 'work together to jointly address growing network and information security threats'. It expressed 'concern over the threat of using [information technology] for purposes inconsistent with the tasks of protecting international stability and security'. An SCO seminar in June has already raised the idea of creating a 'unitary Eurasian information space'[75] (an SCO Internet?).

In 2009, the SCO formally agreed a treaty on the subject.[76] This was the first international treaty on information security that specifically addressed the range of issues that had been canvassed in the annual UN resolutions 'in the context of international security' since the expanded version of 1999. Article 3 of the 2009 treaty commits the parties to cooperate to eliminate a wide range of threats; and 'to work up collective measures for the development of international legal norms in the area of limiting the proliferation and application of information weapons that create

71 United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security,* A/61/161.

72 Bangladesh, Canada, European Union, India, Mongolia, New Zealand, Pakistan, Sri Lanka, and Timor-Leste.

73 'ASEAN Regional Forum, Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyberspace' (The Thirteenth ASEAN Regional Forum 2006, Kuala Lumpur, 28 July 2006), http://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html.

74 *Bishkek Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation* (16 August 2007), http://www.sectsco.org/EN123/show.asp?id=92.

75 See Shanghai Cooperation Organization, *Chronicle of main events at SCO in 2007*, 31 December 2007, http://www.sectsco.org/EN123/show.asp?id=97.

76 Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation*.

threats to defence preparedness, and national or collective security'. Annex 2 over three pages describes five categories of threat:

- Development and use of information weapons, and the preparation and conduct of information war;
- Information terrorism;
- Information crime;
- Use of a dominant position in information space to harm the interests and security of other countries; and
- Spreading of information impacting negatively on the socio-political and socio-economic systems, spiritual, moral and cultural environment of other countries.

Annex 1 carries definitions of 13 basic concepts, among which the most important is the overarching concept of 'international information security', defined as the 'maintenance of international relations excluding the breach of peaceful stability and the creation of a threat to the security of states and world society in the information space'.

Also in 2009, China and ASEAN signed a framework agreement on network and information security emergency response,[77] as a follow-up to their agreement in 2005 on ICT cooperation for development (the Beijing Declaration) and a related agreement in 2007.[78] The 2007 agreement had also set up an ASEAN-China experts group on network security. The two sides commenced an annual seminar on network security in 2009, meeting for the first time in China.

In 2010, China published a White Paper on the Internet in China, an event that came a full fifteen years after the technology began to be introduced into the country outside of its universities.[79] One of the primary motivations for publishing the White Paper was to set out the public values around use of the Internet. The White Paper affirms freedom of speech, democratic supervision of government policies and the citizens' constitutional right to know. In one of six main sections, China discussed its commitment to collaborate internationally in cyber security, referencing a number of its activities mentioned above.

It was in this 2010 White Paper that China staked out a more comprehensive vision of international order concerning the Internet. It said 'China supports the establishment of an authoritative and just international internet administration organisation under the UN system through democratic procedures on a worldwide scale'. It said China was looking for all countries to 'have equal rights in participating in the administration of the fundamental international resources of the

77 China-ASEAN Coordination Framework for Network and Information Security Emergency Responses. See 'The Internet in China,' *English.news.cn*, June 8, 2010, http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232_8.htm. Text of this agreement does not appear to be readily available.

78 See Association of Southeast Asian Nations, *Plan of Action to Implement the Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development*, http://www.asean.org/news/item/plan-of-action-to-implement-the-beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-2.

79 China.org.cn, *Active International Exchanges and Cooperation*, http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207975.htm.

internet', with a 'multilateral and transparent allocation system' to be established 'on the basis of the current management model'. It noted that the 'development of the internet industry brings with it a series of new scientific and moral problems'. It reaffirmed that China would share with other countries the 'opportunities brought by the development of the Chinese Internet industry', 'unswervingly stick to its opening-up policy, open the Chinese internet market in accordance with the law, welcome enterprises from other countries to enter the Chinese internet market', continue to abide by its general obligations and specific commitments as a WTO member, and 'protect the legitimate rights and interests of foreign enterprises in China'.

In 2010, a new UN GGE, constituted one year earlier with China participating, reached important agreements. First, on the threats, it concluded that there is 'increased reporting that states are developing ICTs as instruments of warfare and intelligence, and for political purposes'; and that 'uncertainty regarding attribution and the absence of common understanding regarding acceptable state behaviour may create the risk of instability and misperception'.[80] The GGE made the following recommendations 'for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions':

- Further dialogue among states to discuss norms pertaining to state use of ICTs, to reduce collective risk and protect critical national and international infrastructure;
- Confidence-building, stability and risk reduction measures to address the implications of state use of ICTs, including exchanges of national views on the use of ICTs in conflict;
- Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;
- Identification of measures to support capacity-building in less developed countries; and
- Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.[81]

In addition, the APEC Working Group on Telecommunications agreed in 2010 an action plan for 2010-2015 in which one of five streams was devoted to a 'safe and trusted ICT environment', with a focus on domestic policies: capacity-building, cyber security awareness, security initiatives with industry, safer online environments, and promotion of the Internet economy.[82]

80 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010), 7, http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

81 Ibid, 8.

82 'TEL Strategic Action Plan: 2010-2015, 2010/TELMIN/024' (Asia-Pacific Economic Cooperation, 8th Ministerial Meeting on Telecommunications and Information Industry, Okinawa, 30-31 October 2010), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2010_tel/ActionPlan.aspx.

China's preparedness to collaborate in international rule making for security in cyberspace was demonstrated when it supported the clause in the 2010 Beijing Convention calling on states to criminalise 'technical attack' on aircraft in flight or air traffic control systems.[83]

In January 2011, the US and China committed for the first time a Head of State level to work together on a bilateral basis on issues of cyber security, but this was a passing mention in a set of more than twenty additional issues listed in one long sentence that were judged less important than the substantial number already covered in the statement with some elaboration.[84] This relatively low public prominence for cyberspace issues belied the high importance that both sides privately attached to them, not least in China's case after the revelations the previous year about the US use of the Stuxnet worm. For the US, there was a rising concern about China's use of cyber espionage, especially activities that threatened the safe functioning of its national critical infrastructure.

In a 2011 speech to UN, China's disarmament ambassador Wang Qun acknowledged the transformative aspect of the influence of ICT on security: 'information and cyberspace security represents a major non-traditional security challenge confronting the international community. Effective response to this challenge has become an important element of international security'.[85] Use of the term 'non-traditional' has been a device used by Chinese leaders and officials to avoid giving the impression that the information age has totally transformed the traditional approaches to security. He went on to say that the international community should view this issue from the new perspective of 'a community of common destiny' and 'work together towards a peaceful, secure and equitable information and cyber space'. We can probably assume that this approach contrasts quite strongly with that of mainstream military strategists in China. (It is equivalent to the shift by the Soviet Union under Gorbachev to the idea of common security, a shift that was essential for ending the Cold War.) Wang advocated five principles, as set out in Table 3.

Of some note, Wang directly appealed for the rules of the road, a call heard earlier in the year from the US. Wang said:

> '[I]n this virtual space where traffic is very heavy, there is, hitherto, no comprehensive 'traffic rules'. As a result, 'traffic accidents' in information and cyberspace constantly occur with ever increasing damage and impact. Therefore, the development of international norms and rules guiding the activities in information and cyberspace has become an urgent task.'[86]

83 *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*.

84 For related information, see Greg Austin and Franz-Stefan Gady, 'Cyber Detente between the United States and China,' *EastWest Institute* (2012), http://www.ewi.info/sites/default/files/ideas-files/detente.pdf.

85 'Speech by H.E. Ambassador Wang Qun at the First Committee of the 66th Session of the GA on Information and Cyberspace Security' (The First Committee of the 66th Session of the GA on Information and Cyberspace Security, New York, 20 October 2011), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t869580.shtml.

86 Ibid.

Table 3. China's normative principles for cyberspace (2011).

Peace War avoidance, active preventive diplomacy, and promote the use of information and cyber technology in maintaining security; commit to non-use of information and cyber technology for hostile actions and non-proliferation of information and cyber weapons; while retaining the right of self-defence against 'threats, disturbance, attack and sabotage'; prevent a cyber arms race and settle disputes peacefully.
Sovereignty States remain the main actor in governance of information and cyberspace; sovereignty and territorial integrity remain basic norms; countries should build a comprehensive and integrated national management system for all aspects of cyberspace; cyber technology should not be used as 'another tool to interfere in internal affairs of other countries'.
Balance between freedom and security Uphold the rule of law to keep order in information and cyberspace; practicing power politics in cyberspace in the name of cyber freedom is untenable.
Cooperation Interdependence of cyber networks ('interlink with each other and belong to different sovereign jurisdictions') means that 'no country is able to manage only its own information and cyber business' or 'ensure its information and cyber security by itself'; all countries need to work together.
Equitable development Developed countries have an obligation 'to help developing countries enhance capacity in information and cyber technology and narrow the digital divide'.

In 2011, in order to promote such a policy agenda on the international stage, China and several other countries (Russia, Tajikistan and Uzbekistan) submitted to the United Nations General Assembly a proposal for an International Code of Conduct for Information Security.[87] The draft code calls on states to observe international law as set out in the UN Charter as well as 'universally recognised norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all states'. The code also calls on states 'not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies'.

Russia was the driving force behind this, not China, but it nevertheless represented a new level of international mobilisation by China. These proposals go close to matching those previously elaborated by Chinese representatives. This idea of common security received further expression in 2012 (not referencing information security in particular) in a speech by Vice Minister of Foreign Affairs Cui Tankai to the Asia Society in Hong Kong: 'we believe countries should build mutual trust and seek common security … Security at the expense of others will only make us less secure'.[88]

87 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), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement.

88 Wendy Tang, 'Cui: Toward 'Common Security' and Cooperation in the Asia Pacific,' *Asia Society*, July 5, 2012, http://asiasociety.org/hong-kong/cui-toward-common-security-and-cooperation-asia-pacific/.

In August 2011, a political commentator from the Chinese National Defence University observed:

> 'I think that first we should follow the basic norms of the Charter of the United Nations and other internationally recognised norms, establish and improve cyberspace theory around national interests and sovereignty with Chinese characteristics, build our own network warfare theory, develop a cyberspace policy and legal system with our own characteristics, and in the world support the principle of building a harmonious cyberspace.'[89]

In October 2012, a Chinese diplomat elaborated the same point differently, including a direct invocation of existing international law:

> 'Peaceful use of cyberspace benefits the interests of every country and the common interests of mankind. We call upon all countries to observe the UN Charter and universally recognised international laws and norms governing international relations, not to take advantage of their internet technologies and resources to jeopardise the national security of other countries, not to conduct hostile activities against other countries or threaten international peace and security, and not to research, develop or use cyber weapons.'[90]

Work on the Code of Conduct between Russia and China had proceeded in tandem with a series of discussions in various forums in 2012 on a draft UN Convention on Information Security which had been prepared by a group of Russian experts. China was actively involved in several of these forums to discuss the draft.[91] Track 2 discussions on China's approach to international legal norms for cyberspace also became more focused and productive by 2012, showing areas of agreement and disagreement between unofficial representatives of China and the US.[92]

In March 2013, China had to deal with an unusually robust set of public demands on it to curtail what the US saw as its malicious activities in cyberspace. The US National Security Adviser, Thomas Donilon, called on China to undertake a bilateral dialogue with the US to establish 'acceptable norms of behaviour in cyberspace'.

In June 2013, the GGE, with a Chinese representative participating, reached consensus that the rules of international law do apply in cyberspace and called for more development work on future norms and the promotion of confidence

89 Liu Zenglian, 'How to Build the Network Border Defense,' *People's Forum*, August 19, 2011 [in Chinese].

90 'Statement at Budapest Conference on Cyber Issues' (Huang Huikang, Budapest Conference, Budapest, 4 October 2012), http://www.chinesemission-vienna.at/eng/zgbd/t977627.htm.

91 Anastasia Matvejeva, 'The Concept of Freedom is Not Absolute,' *Gazeta.ru*, February 9, 2012, http://www.gazeta.ru/business/2012/02/09/3994965.shtml [in Russian].

92 There were several forums for such meetings, including those organised between US think tanks and a range of counterparts in China. Those organised (separately) by the EastWest Institute and the Centre for Strategic and International Studies (CSIS) had begun in 2009. Those conducted by the EastWest Institute included contacts with the Central Military Commission, at the time China's highest decision-making body in strategic policy. The summary report of the CSIS meetings in 2012 is particularly illuminating. See Center for Strategic and International Studies (CSIS), *Bilateral Discussions on Cooperation in Cybersecurity*.

building.[93] The GGE also called out what this meant in terms of the application of norms of sovereignty, human rights and state responsibility. Key excerpts are here *verbatim*:

- 'The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability'.
- 'Common understandings on how such norms shall apply to State behaviour and the use of ICTs by States requires further study'.
- 'Given the unique attributes of ICTs, additional norms could be developed over time.
- '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'.
- 'State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'.
- 'State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments'.
- 'States should intensify cooperation against criminal or terrorist use of ICTs, harmonise legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies'.
- 'States must meet their international obligations regarding internationally wrongful acts attributable to them'.

In the debate in the First Committee in October 2013, China's delegate presented an enriched picture of Chinese threat perception by referencing pre-emptive military strike while referring to earlier ideas, such as some countries using their dominant position in cyberspace to interfere in internal affairs of others, export controls on ICTs, and militarisation by some countries of cyberspace.[94] He reiterated the idea of common security: 'Cold War mentality and zero sum game theory is neither feasible nor tenable in the information space'. He advocated four principles and three measures.

93 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 the Secretary-General*, A/68/98 (24 June 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

94 'Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 65th Session UNGA' (United Nations, New York, October 2013), http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf.

The principles were familiar:

- States should observe the UN Charter and not threaten each other in cyberspace;
- States should not use ICT dominance to interfere in other states affairs;
- There should be equitable and democratic governance of the Internet; and
- States should promote exchange of ICT for peaceful development across the digital divide.

The three measures were:

- '[D]evelop a set of universal and effective international norms and rules governing activities in information space';
- Make full use of the GGE to 'deepen mutual understanding and explore the international norms and rules'; and
- '[G]ive play to the leading role of governments', who have a leadership role domestically in stimulating private-public initiatives and multi-stakeholder approaches, while at the international level to drive cooperation in combating cyber crime and cyber terrorism, and in protecting critical information infrastructure.

The delegate then observed that China had an exemplary record in promoting global cooperation through its work in various global and regional organisations.

7. China Resets Its Cyber Ambitions 2014–2015: Norm Entrepreneurship Will Change

Starting from 2014, the pace of China's efforts around international legal norms in cyberspace has been the most intense since China joined the global information economy in 1993.[95] The quickening of pace can be traced to February 2014, when President Xi Jinping declared that China would do everything necessary to become[96] a cyber power and that there could be no national security without cyber security.

Key policy developments that demonstrate Xi's earnestness have been his call in September 2014 for China to develop a military strategy for cyberspace, and the delivery of elements of such a cyber concept (in broad terms) in May 2015 in

95 This is the year China set up its first national body for the information economy, a technocratic policy group which eventually transformed itself through several iterations, expansion and political upgrading into the Central Leading Group for Informatisation and Cyber Security, a leadership group of the Communist Party and the State Council formally (re)constituted in 2014 and chaired by President Xi Jinping.

96 Zhu Ningzhu, ed., 'Xi Jinping Leads Internet Security Group,' *English.news.cn,* February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

'China's Military Strategy',[97] the first official document of its kind released in public with that title. The depth of the commitment was also revealed in a governmental restructuring to create the Cyberspace Administration of China, an organisation that was assigned to support the freshly reorganised Central Leading Group on Informatisation and Cyber Security, upgraded by Xi when he took it over at the time of the 'cyber power' announcement. We could reasonably conclude that these moves might have been accompanied by some adjustment in China's approach to international legal norms for cyberspace. For example, if China was now committed in public to joining the ranks of military cyber power powers, one might have expected its position to shift more toward accommodating the views of other major cyber military powers.

As this chapter was being completed, China played its strongest card yet in the diplomacy of cyber norms. In early September 2015, it sent the Politburo member with responsibility for China's non-military spy agencies, Meng Jianzhu,[98] to Washington for four days for official discussions to try to dampen controversies with the US about the norms of cyber espionage in advance of a state visit by President Xi Jinping.[99] This was the high point in direct official contact on the subject resulting from a robust diplomatic campaign by the US which reached a peak in March 2013 when National Security Adviser Thomas Donilon made public demands on China to abide by rules of the road prohibiting cyber espionage for commercial purposes.[100]

Just weeks earlier, the United Nations published the report of the fourth Group of Governmental Experts (GGE) on certain aspects of information and telecommunications affecting international security.[101] With Chinese representation in the GGE, this report marked a new high point in intergovernmental consensus on some related issues, including most importantly the endorsement of a range of possible 'voluntary, non-binding norms, rules or principles' for restraint in international cyber practices.

The 2015 GGE report reached an agreement on three important and potential 'voluntary non-binding norms' for state behaviour in cyberspace:

97 The State Council Information Office of the People's Republic of China, *China's Military Strategy* (May 2015), Beijing, http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm.

98 Of special note, Meng controls the civilian spy agencies (Ministry of State Security for external intelligence and Ministry of Public Security for domestic intelligence). He does not control the main signals intelligence agency of China which sits in the People's Liberation Army, under the control of the Central Military Commission of the Chinese Communist Party (CCP). Meng is the Secretary of the Central Political and Legal Commission, one of the most powerful political bodies in the country because of its role is the protection of all aspects of the 'political and legal' system in the country.

99 The White House, Office of the Press Secretary, *Readout of Senior Administration Officials' Meeting with Secretary of the Central Political and Legal Affairs Commission of the Communist Party of China Meng Jianzhu*, 12 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/12/readout-senior-administration-officials-meeting-secretary-central.

100 Greg Austin, 'Cybersecurity: The Toughest Diplomatic Challenge Is China's Weakness,' *The Global Journal*, April 5, 2013, http://theglobaljournal.net/article/view/1049/.

101 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), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

- States should not attack each other's critical infrastructure for the purpose of damaging it;
- States should not target each other's cyber emergency response systems; and
- States should assist in the investigation of cyber attacks and cyber crime launched from their territories when requested to do so by other states.[102]

These proposals represented important refinements of previous Chinese positions in UN forums in providing that states should be held accountable for acts that were more precisely defined than simply being against the UN Charter principles. At the same time, all three of these proposed norms had been foreshadowed in China's diplomatic activity in some way, principally in APEC beginning of 2001, with ASEAN after 2003, and in China's support for the formation of the Asia Pacific Computer Emergency Response Team (APCERT) in 2003 (at a meeting in Taipei).

In the first half of 2015, China made three other important advances in its approach to international legal practice for cyberspace. First, on 8 May, it concluded a formal agreement with Russia not to interfere unlawfully in each other's information resources and networks.[103] Second, China and the US agreed to negotiate a 'code of conduct' of some kind in cyberspace.[104] Third, though less important, in January, China had participated in tabling a slightly revised draft of the proposed code of conduct for cyberspace initially submitted to the United Nations in 2011.[105]

By signing the new bilateral agreement in May, China and Russia together appear to have pre-empted the advisory effect of the GGE report, and its recent predecessors, to give legal effect to some of the principles proposed. The bilateral agreement goes very close to constituting a formal military alliance in cyberspace, since it lays out a mutual obligation of assistance in the event of a wide range of cyber attacks.

The Russia/China agreement is the fulfilment of a decade of involvement by the two countries in cooperative measures on cyberspace governance, including through the Shanghai Cooperation Organization talks beginning in 2006. The new agreement formalises at a bilateral level the countries' proposal in the UN system for a code of conduct in cyberspace. The agreement is as much about that effort as it is about strengthening each other in the face of US cyber pre-eminence. Article one describes malicious use of cyberspace 'as a fundamental threat to international

102 Ibid.

103 For a text of the approved agreement, see Government of the Russian Federation, *Order of the Russian Government on signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China*.

104 The US Secretary of State, John Kerry, announced on 23 June 2015 the following: 'We believe very strongly that the US and China should be working together to develop and implement a shared understanding of appropriate state behavior in cyberspace, and I'm pleased to say that China agreed that we must work together to complete a code of conduct regarding cyber activities.' See John Kerry, U.S. Department of State, *The Strategic & Economic Dialogue / Consultation on People-to-People Exchange Closing Statements* (Washington DC: 2015), http://www.state.gov/secretary/remarks/2015/06/244208.htm. While Kerry implies that this was a US proposal, it appears to have been a Chinese proposal, flagged in the opening remarks several days earlier by China, rather than a US proposal, and it had been China's policy since 2011 at least.

105 See 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.

security'. Article 4 only commits the two countries not to undertake actions like 'unlawful use or unsanctioned interference in the information resources of the other side, particularly through computer attack'.

This is not a commitment to refrain from all use of military cyber assets against each other. Article 4 only says that each country has an equal right of self-defence in cyberspace against 'unlawful use or unsanctioned interference in the information resources of the other side, particularly through computer attack'. Neither Russia nor China regards cyber espionage or preparations for war in cyberspace as 'unlawful' or 'unsanctioned'. Of some note, Article 6.2 commits both parties to protect the state secrets of the other in cyberspace, and references a prior bilateral treaty with that general effect dating from 24 May 2000. The Russia/China agreement in its totality may put some pressure on other states to follow suit in the diplomacy of military cyberspace cooperation.[106]

The preamble has extensive new language on the sovereignty principle, with both sides reaffirming that 'state sovereignty and the international norms and principles flowing from state sovereignty, extend to the conduct of states in their use of information and communications technologies and the jurisdiction of states over the information space, and in the same way, a state has sovereign rights to define and undertake state policy on questions connected with the information and telecommunications network of the Internet, including the maintenance of security'.

It should be noted that the idea of a 'code of conduct' long advocated by China and Russia is just another way of laying down a set of voluntary non-binding norms of the kind agreed by the GGE in 2015. In sharp contrast, the 2015 agreement with Russia delivers to China an alliance relationship to buttress its information security and support its capacity development as it keeps its sights on Xi's goal of China becoming a cyber power. Furthermore, as I have often argued, China's interests in economic security aspects of cyberspace may now be driving it to some accommodation with the US on normative behaviours. Thus, between 2014 and 2015, China could feel it was making headway both in its political contest with the US over cyber norms and in its quest to become a cyber power even if that meant winning some diplomatic battles and losing others.

8. Conclusion

China's approach to international legal norms for cyberspace has not changed fundamentally at least since 2002 when the country made its first major statement

106 The agreement followed a Japan-US agreement on cyberspace cooperation in military affairs. Japan Ministry of Defense, *Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group*, 30 May 2015, http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf.

on the subject in the UN General Assembly. There has been useful elaboration by China on some of the detail, especially concerning protection of critical infrastructure and emergency response, which contributed to the meeting of minds in the UN GGE in 2015.

One important change has been in China's sense of urgency in using such norms to restrain countries like the US from more rapid strengthening of what China sees as the US hegemonic position in cyberspace. The cause of this change is China's deepening sense of insecurity in cyberspace, both domestically and on the international stage. Even though the place of espionage in China's exploitation of cyberspace has also expanded dramatically since 2002, this represents no change in its approach to international legal norms for cyberspace. China's interests in international cooperation to protect critical cyber infrastructure and, separately, to counter terrorism in cyberspace have deepened. At the same time, China has been sending conflicting signals about how to strike a balance between sovereign rights for control of sensitive cyber technologies in the name of national security and norms that allow for continued deep integration in a globalised ICT industry and a global cyberspace. China's interest in using advanced ICTs, especially for domestic political control has deepened enormously, and this carries important implications for its positioning on international legal norms in cyberspace.

China's main international security concerns have been military cyber conflict and foreign interference in Chinese domestic networks for the promotion of political dissent. China's position has largely been one about which norms should apply and in what circumstances, while emphasising the need for discussions about new normative behaviour and possible new norms, including a possible code of conduct or treaty that is specific to the action of states in cyberspace. While recognising that the normative position China takes on certain issues (its interpretation of international law) is ethically distinguishable from those taken by the US and like-minded countries, or from those that various scholars including me might take, suggestions that China has not been prepared to engage or promote new norms, or that such negotiations must be a zero sum game,[107] are not ones I would support. Moreover, we need to recall that the normative differences between the US and the European Union are also significant, if not perhaps as big as those between the US and China.

There have been multiple sources of confusion about China's position: under-appreciation of the overriding importance to China of existential security needs in cyberspace; lack of clarity in discussion by Chinese participants in Track 2 meetings, and even in the GGE, between international legal norms and other norms; reliance on unofficial interlocutors who, while working for the Chinese government, have few qualifications to represent a formal view of the Chinese government; and

107 See for example James A. Lewis, *Cyber War and Competition in the China-U.S. Relationship* (China Institutes of Contemporary International Relations, 2010), http://csis.org/files/publication/100510_CICIR%20Speech.pdf.

mistaking norm entrepreneurship (and its relentless propagandistic pursuit) in military affairs as the totality of China's position. A state's position on an international legal norm is only what the state's plenipotentiary representatives say it is.

By September 2015, there are increasing signs that China feels obliged to cooperate in cyberspace rather than risk the fabric of its economic ties. China's economy is almost certainly not immune from serious damage that could be brought on by a US cyber attack. In both countries, elements of the civil infrastructure dependent on the cyber domain (mobile communications, Internet, electricity grids, land lines, undersea cables, banking) are inter-mingled with military assets. In most countries, the mingling is so profound that it is called 'entanglement'. In broad terms, this characteristic is shared with all countries. But exactly just how this entanglement, and its impact on China's normative behaviour looks from Beijing's perspective is worthy of much deeper study.

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

CHAPTER 10

Technological Integrity and the Role of Industry in Emerging Cyber Norms

Ilias Chantzos and Shireen Alam

1. Introduction

This article explores the development of cyber norms and illustrates how the cyber security industry cooperates with government agencies and institutions to address an array of cyberspace issues. The discussion then focuses on the development of the principle of technological integrity, an issue which has arisen in the wake of arguments against the weakening of encryption through the installation of hidden functionality in software and hardware products. Symantec is committed to the principle of technological integrity as a critical cyber norm. The article explains some of the key benefits to be derived from technological integrity, as well as the risks if it is not observed. It concludes by laying out a number of recommendations, such as the importance of technological integrity as a norm, the need to develop feasible requirements, the need to remain open to alternative policy options, and the need to balance cyber security and national security.

The article also emphasises that governmental institutions benefit from having the perspectives of the private sector, especially since industry as the primary technology innovator and provider has a greater impact on cyber norms development and consequences than perhaps on norms in other fields.[1] In that regard the

1 Matt Thomlinson, 'Advancing the Discussion on Cybersecurity Norms,' *Microsoft Cyber Trust Blog*, October 21, 2013, https://blogs.microsoft.com/cybertrust/2013/10/21/advancing-the-discussion-on-cybersecurity-norms/.

concept of building cyber norms is unique to the creation of other types of norms. In this article, Symantec applies an overarching approach as it views cyber norms as explicit, agreed on principles, rules of behaviour, procedures, or codes of conduct, that are not necessarily legally binding.[2]

Technological integrity is a principle that promotes privacy measures and shuns the prospect of hidden functionality. Law enforcement agencies around the world are battling against widespread encryption and asserting that a lack of backdoors is causing criminal – including terrorist – investigations to 'go dark'.[3] However, it is nearly impossible to have the luxury of strict security together with surveillance, since beyond a certain point the ability to survey erodes security.[4] In turn, this means that there remains no option for governments to have spying capabilities without creating this opportunity to criminals.

Leading cryptographers have deemed hidden functionality to be unworkable, citing factors including security, feasibility, cost, credibility, and economic repercussions as well as legal and ethical entanglements.[5]

2. Cyber Norms

For the purposes of this article, cyber norms are defined as generally accepted principles of cyber behaviour which set a framework for discussion. They are regarded as inclusive as well as flexible in providing greater options, and they progressively change mind-sets and behaviours.[6] Norms are changeable and capable of strengthening or weakening over a period of time.[7] Cyber norms evolve through policies, products and patterns of behaviour in gaining social acceptance and thus become convention. They can be formalised or enforced through more specific legally binding norms or policy agreements both on the domestic and international levels.

In contrast to the historical evolution of international norms, the development of cyber norms should engage the private sector. While it remains true that only

2 Richard A. Clarke, *Securing Cyberspace through International Norms Recommendations for Policymakers and the Private Sector* (Washington D.C.: Good Harbor Security Risk Management, 2013), 7-10, http://www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf.

3 Joshua Kopstein, 'The Feds Don't Need Digital Backdoors – They Can Hack You,' *Aljazeera America*, July 17, 2015, http://america.aljazeera.com/opinions/2015/7/the-feds-dont-need-digital-backdoors-they-can-hack-you.html.

4 Bruce Schneier, 'What is the DoD's Position on Backdoors in Security Systems?' *Schneier on Security*, June 24, 2015, https://www.schneier.com/blog/archives/2015/06/what_is_the_dod.html.

5 Harold Abelson, *et al,* The Massachusetts Institute of Technology, *Computer Science and Artificial Intelligence Laboratory, Keys Under Doormats*: *Mandating Insecurity* by *Requiring Government Access* to *all Data* and *Communications: Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2015-026 (6 July 2015),* https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

6 Royal United Services Institute, *Cyber Norms of Behaviour: Executive Summary* (15 March 2015), https://www.rusi.org/downloads/assets/Cyber_norms_of_behaviour_report_-_Executive_Summary.pdf.

7 Tim Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-Security? Discussion Paper 2011-11* (Cambridge, Mass.: 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.

nation states can create legally binding norms, the role of industry is unique as a significant amount of the infrastructure of the Internet is privately owned.[8] For example, the private sector has helped to develop agreements such as the Financial Action Task Force on Money Laundering[9] and was also indispensable in securing parliamentary support for its ratification.[10] Similarly, in Europe, the private sector has been consistently consulted by policy-makers in charge of developing and furthering the European Union's policies on network and information security, such as through the European Public-Private Partnership for Resilience[11] and the European Network and Information Security Platform.[12]

Some concrete ways in which the cyber security industry plays a role in influencing cyber norms include: 1) developing the latest technologies and their use; 2) monitoring and informing on the evolution of the threat landscape; 3) engaging in Public Private Partnerships (PPP) and capacity-building efforts; 4) assisting law enforcement in fighting cyber crime; and 5) providing technologies and scalable capabilities to enable countries to implement regulations and public policies.

2.1 Developing Technologies and Use

The cyber security industry plays a pivotal role in developing norms through its products and services markets.[13] It will continue to be involved in the development of norms because of its role in ultimately conceiving of and building products, services, and infrastructure that enable the digital world. Groups focusing on advancing Internet technologies and standards offer good examples of the development of informal international norms through their scale and footprint across international product markets.[14]

Technology is implemented in the context of existing cultures, customs and laws and plays a key role because it determines how norms evolve. In a way, the relationship between norms and technology is interdependent and mutually influential. Due to the constant evolution of technology and the emergence of new practices and behaviours which they enable in cyberspace, new norms are needed to address challenges on the international stage between countries.

The valuable expertise that the private sector carries bestows upon the sector an added advantage in setting technical as well as performance-based standards. By setting high standards for security products, the private sector can set the criteria for

8 Microsoft Corporation, *Five Principles for Shaping Cybersecurity Norms* (2013), http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Five_Principles_Norms.pdf.

9 FATF is an intergovernmental organization established by the G7 in Paris and its membership consists of 36 nations which makes policies for combating money laundering, terrorist financing and other matters related to the integrity of the international financial system.

10 Clarke, *Securing Cyberspace through International Norms Recommendations for Policymakers and the Private Sector.*

11 European Union Agency for Network and Information Security, 'European Public Private Partnership for Resilience (EP3R),' https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

12 European Union Agency for Network and Information Security, 'NIS Platform,' https://resilience.enisa.europa.eu/nis-platform.

13 Royal United Services Institute, *Cyber Norms of Behaviour: Executive Summary.*

14 Ibid.

the level of security we can expect. A prime example of this is the Software Assurance Forum for Excellence in Code (SAFECode) of which Symantec is a founding member. SAFECode develops guides for software assurance within its community, which includes some of the largest software providers in the world. In doing so, it provides industry leadership on software assurance as well as clarity on the applicable best practices and recommendations for assuring security, reliability and confidence in the security of software that is purchased.[15]

2.2 Creating Threat Awareness

According to the annual Symantec Internet Security Threat Report (ISTR), there were 317 million new pieces of malware in 2014, or nearly one million new malware variants per day. Social media was confirmed as the fastest-growing vector for malware proliferation.[16] Due to their worldwide coverage, private sector operators are better positioned than most national governments to develop comprehensive near real-time threat awareness. They are also able to share timely and relevant information with appropriate public agencies across multiple jurisdictions, and this proves to be a crucial asset for many nations and their alliances in developing and maintaining their cyber defence postures.

2.3 Public-Private Partnerships and Capacity-Building

Public-Private Partnerships (PPP)[17] and capacity-building[18] are essential elements in the eventual development of cyber norms.[19] A key minimum requirement in the development of norms is consensus, or at least a common understanding among states about the nature of the problem and the need for it to be resolved in a particular way. Capacity-building creates and increases skills, experience, knowledge, and ultimately helps states and other organisations to understand the technological problem and to recognise the need for effective cyber security. PPPs provide much-needed information and help build the necessary expertise at the local level that makes the application and enforcement of norms possible.

Deeper collaboration between the private and public sectors is a crucial asset in cyber security endeavours. Government agencies at all levels should form meaningful partnerships with the private sector. A single player does not have all the answers, resources, skills, assets or scalable capabilities to counter rapidly growing

15 Shaun Gilmore, et al, *Principles for Software Assurance Assessment. A Framework for Examining the Secure Development Processes of Commercial Technology Providers* (*Software Assurance Forum for Excellence in Code* (SAFECode), 2015), http://www.safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf.

16 The ISTR is the Symantec annual report that analyses a year of observations captured over the Symantec Global Intelligence Network, a set of over fifty million sensors spread over the Internet in more than 150 Countries. The full report and supplemental data are available at Symantec, *The 2015 Internet Security Threat Report (ISTR20)*, vol. 20 (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

17 PPP is a joint government and private venture as it is funded and run through the government as well as a private sector or multiple private companies.

18 Capacity-building is the strengthening and enhancing of skill sets to enable communities as well as organizations to flourish and help keep up with developments and changing times.

19 'Capacity Building in Cyberspace: Taking Stock' (Event Report, European Union, Institute for Security Studies, A seminar organised in the framework of the EUISS Cyber Task Force, Brussels, 19 November 2013), http://www.iss.europa.eu/uploads/media/EUISS_Cyber_Task_Force_Report.pdf.

and evolving cyber threats. Therefore, it is in the interests of all parties to foster different collaboration models that enable the exchange of information, as well as the dissemination of expertise and capacity-building. PPPs serve a vital function as they can facilitate knowledge and capability transference, alleviate shortages of skilled cyber security professionals through collaborative work, and enable real time exchange of cyber threat information.[20]

Capacity-building is not only limited to developing technical skills, but also requires a broader understanding of the technology, policy and threat environment. Without this knowledge, policy-makers are not well equipped to make fully informed decisions. For example, international organisations like the International Telecommunication Union (ITU)[21] and the Organization of American States (OAS)[22] have entered into partnerships with companies to disseminate information to their members on the current threat landscape with an emphasis on particular regions or issues. The objective is to ensure that knowledge on cyber security matters is shared and to build a common understanding among the member nations' policy-makers.

Thus, the contribution of the cyber security industry in the development of national and regional policies creates a local framework in which norms are established and helps ensure their practical implementation. PPPs support capacity-building and policy development by helping states to be better informed and to debate various types of norms. Despite the different stages of technological maturity and various legal and political cultures, an improved common understanding about the nature of cyber security challenges raises the likelihood of reaching consensus on how cyber norms need to reflect that understanding.

2.3.1 Assistance to Law Enforcement in Fighting Cyber Crime

It has been acknowledged that only a decentralised governing method of the cyber domain will present a successful approach.[23] The areas of cyber crime and law enforcement contain the greatest potential for international collaboration in creating cyber norms. For example, although the Budapest Convention[24] is regarded by many states as the international benchmark for combatting cyber crime, its status as a Council of Europe instrument places limits on the extent of its influence globally. It has been suggested by some that a possible avenue to address and resolve this would be to draft a new instrument, which encompasses international issues for all states based on the Budapest Convention.[25]

20 Frederick Wamala, International Telecommunication Union, *The ITU National Cybersecurity Strategy Guide* (September 2011), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

21 International Telecommunication Union, 'Global Partnerships with Industry Players,' http://www.itu.int/en/ITU-D/Cybersecurity/Pages/symantec_and_trend_micro.aspx.

22 Organization of American States, Press Department, *OAS and Symantec to Present Cyber Security Report on June 2nd*. AVI-100/14, 28 May 2014, http://www.oas.org/en/media_center/press_release.asp?sCodigo=AVI-100/14.

23 James Jay Carafano and Eric Sayers, *Building Cyber Security Leadership for the 21st Century*, No. 2218 (Washington D.C.: The Heritage Foundation, 2008), http://www.heritage.org/research/reports/2008/12/building-cyber-security-leadership-for-the-21st-century.

24 *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.

25 Royal United Services Institute, *Cyber Norms of Behaviour: Executive Summary.*

Using the common understanding of what constitutes cyber crime that the Budapest Convention provides allows industry to collaborate extensively across different jurisdictions with law enforcements agencies. These operations are often newsworthy and focus against organised cyber crime in infrastructure takedown. For instance, Symantec has formal partnerships with law enforcement organisations around the world including Europol, and participates with several other companies in sharing information on infrastructure used by cyber criminals. It then participates in the process of taking down that infrastructure, thus assisting law enforcement and protecting its customers and the broader community.[26]

2.3.2 Development and Implementation of Public Policies

The cyber security industry has been actively involved in the development of public policies through a number of mechanisms including public consultations. Industry experts are regularly invited to provide policy recommendations as well as functional and technical expertise. In particular, the cyber security industry is often asked to assess policy recommendations, and to provide input on the technical feasibility and practical impact of future policies.

Some recent examples where the cyber security industry has been invited to provide expertise, business perspectives and best practices to policy-makers include the European Union General Data Protection Regulation (GDPR),[27] the Network and Information Security (NIS) Directive,[28] the European cyber security strategy,[29] the European Regulation on Electronic Identities and Trust Services (eIDAS),[30] and the Directive on Attacks Against Information Systems.[31]

Cyber security experts participate in advisory roles for international agencies and organisations which are active in cyber security matters. For instance, the statutes of the European Network and Information Security Agency (ENISA) of the European Union[32] created the Permanent Stakeholder Group (PSG) appointed

26 'Ramnit Cybercrime Group Hit by Major Law Enforcement Operation,' *Symantec Connect*, February 25, 2015, http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation; EUROPOL, *Botnet Taken Down through International Law Enforcement Cooperation*, 25 February 2015, https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation.

27 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM(2012) 11 final (25 January 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

28 European Commission, *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, COM(2013) 48 final (7 February 2013), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN.

29 European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final (7 February 2013), ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

30 European Parliament and Council of the European Union, *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC*, 910/2014 (23 July 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

31 European Parliament and Council of the European Union, *Directive 2013/40/EU on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*, 2013/40/EU (12 August 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l33193&from=EN.

32 European Parliament and Council of the European Union, *Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency*, 460/2004, (10 March 2004), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

every 2½ years to serve in an advisory capacity to the Executive Director with the aim of providing feedback on ENISA's work programme. ENISA's objective consists of improving the cyber security posture across the European single market. ENISA's model of engaging stakeholders from the onset in the decision-making process through preparation of the work programme has proven to be successful.

In addition, the European Cyber Crime Centre (EC3), that sits within the European Police Agency (EUROPOL), has adopted a similar model. The EC3 has different advisory groups which provide advice and support on the exercise of the Agency's mandate. The Internet Security Advisory Group is focused on advising on and facilitating law enforcement action against cyber crime. The EC3 has announced a number of successful operations in collaboration with the cyber security industry that have eliminated criminal infrastructure, such as major botnet takedowns.[33]

The North Atlantic Treaty Organization (NATO) established the Cooperative Cyber Defence Centre of Excellence (CCD COE) in May 2008 and the Centre obtained the status of International Military Organisation in October 2008. The Centre has recognised the compelling need to address emerging challenges on cyber which affect the ability of NATO to achieve its mission and impact the defensive capabilities of NATO nations. Its mission is to enhance cyber defence awareness and security through capability, cooperation and information sharing among NATO member nations and partners.[34] In achieving its mission the NATO CCD COE is partnering with the private sector in activities such as cyber defence exercises.[35]

NATO is also in the process of developing its own cyber security partnership. It initially indicated its readiness to engage with the cyber security industry during the Wales Summit of 2014.[36] The Alliance recognised the importance of working with the private sector in order to better protect NATO and allied infrastructure and to support its ability to conduct operations. A number of activities are already underway focusing on information sharing, capacity-building and promoting technological innovation to address emerging challenges. Within the framework of the NATO cyber security partnership initiatives, Symantec recently signed an agreement with the NATO Communications and Information Agency.[37] The aim of the agreement is to share information on cyber security threats in an effort to develop a collective approach in building trust and defending global networks and critical infrastructure.

The cyber security industry also works with governments to develop standards which meet private and public sector needs. Such collaboration in the United States produced the National Institute of Standards and Technology (NIST) Cybersecurity

33 EUROPOL, *Botnet Taken Down through International Law Enforcement Cooperation*.

34 NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/.

35 North Atlantic Treaty Organization, Allied Command Transformation, *Lock Your Shields and Brace for Impact*, 29 October 2013, https://www.act.nato.int/article-2013-2-3.

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

37 North Atlantic Treaty Organization, *NATO Builds Cyber Alliances*, 11 December 2015, https://www.ncia.nato.int/NewsRoom/Pages/151211_NATO-builds-cyber-alliances.aspx.

Framework, which stems from a Presidential Executive Order released in February 2013 titled, 'Improving Critical Infrastructure Security'.[38] The NIST Cybersecurity Framework consists of guidelines and references to global standards and best practices that help organisations to identify, detect, protect, respond and recover from cyber attacks. The NIST Cybersecurity Framework also creates a common language to ease internal and external communications for cyber security.[39]

3. Emergence of Cyber Norms

Private sector organisations also have been key in supporting human rights norms around Internet freedom. Internet freedom states that existing international human rights standards pertain to the Internet in guaranteeing the right to freedom of expression.[40] An example of this is the Global Network Initiative (GNI), a non-profit organisation composed of various groups including private technology firms, investors, universities, and civil society groups. The GNI has created rules and implementation guidelines for Information and Communication Technologies (ICT) companies to ensure they are supporting the principles of Internet freedom.[41]

A number of non-governmental organisations (NGOs) also engage in the cyber norms discussion. The International Committee of the Red Cross is regarded as an influential non-state promoter of norms on international humanitarian law. The Red Cross has consistently maintained that the law of armed conflict (LOAC) must guide offensive cyber operations.[42] The law of armed conflict prevents unnecessary suffering, and requires proportionality while taking into account military necessity and not impeding on the effective waging of war. The Tallinn Manual (a non-binding document produced by legal and military experts), considered to be an authority on international cyber law, recognises that standalone cyber attacks may constitute armed conflicts depending on the circumstances.[43] If the circumstances fit the criteria then LOAC applies and in a similar manner to a traditional battlefield environment.[44]

38 The White House, Office of the Press Secretary, *Executive Order -- Improving Critical Infrastructure Cybersecurity*, 12 February 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

39 PricewaterhouseCoopers LLP, *Why You Should Adopt the NIST Cybersecurity Framework* (May 2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

40 United Nations, General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, A/HRC/17/27 (16 May 2011), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

41 Clarke, *Securing Cyberspace through International Norms Recommendations for Policymakers and the Private Sector.*

42 Information Technology Industry Council, *The IT Industry's Cybersecurity Principles for Industry and Government* (Washington D.C., Information Technology Industry Council, 2011), http://www.itic.org/dotAsset/191e377f-b458-4e3d-aced-e856a9b3aebe.pdf.

43 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

44 Ibid.

An aspect of the current debate focuses on whether the application of LOAC is needed when cyber attacks like the example below cause significant collateral damage. As the LOAC principles continue to develop, there has been talk of establishing norms for reimbursing harmed private sector corporations that are damaged or disrupted by state activities. The main argument of those supporting the application of LOAC is that states must take responsibility for these costs as currently the private sector bears the costs.

The UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security is comprised of 20 nations that are equitably distributed based on geography, and includes nation states regarded as leaders in the field of cyber. The UN GGE released a consensus report which proposes norms of responsible behaviour and includes commentary on applicable principles of international law.[45] These norms require that a state should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should also take appropriate measures to protect their critical infrastructure from ICT threats. States should not harm the information systems of the authorised emergency response teams of another state or use those teams to engage in malicious international activity. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions.[46] However, attacks on cyber infrastructure by state or non-state actors are illegal under the principles of international law and the UN GGE stated that the UN Charter, including the principles on non-intervention and use of force, are applicable to cyberspace.[47]

The recent consensus achieved at UN GGE has received support from the private sector and is seen as a positive step forward in the norms debate. It should be noted that with regard to the other side of the spectrum (requiring action by countries in defending against cyber damage), nations have been progressively using bilateral, regional or multilateral methods for cyber security towards critical infrastructure. Other countries use the principles of international law directly. It has also been suggested that 'the goal is to consider what norms should apply below the level of armed conflict in cyberspace'.[48]

45 Henry Rõigas and Tomáš Minárik, *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law,* Incyder News, NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

46 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 the Secretary-General*, A/70/174 (22 July 2015), 3, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

47 David Didler, 'Cyber Norm Development and the Protection of Critical Infrastructure,' *Council on Foreign Relations*, July 23, 2015, http://blogs.cfr.org/cyber/2015/07/23/cyber-norm-development-and-the-protection-of-critical-infrastructure/.

48 Ibid.

4. Technological Integrity Principle

There are norms that have achieved a certain degree of consensus, such as those proposed by the UN GGE, as well as other norms emerging in the debate.[49] As technology and public policy challenges continue to develop, it is a normal evolution that norms will need further refinement to address new situations and complexity. The 'technological integrity principle' is an emerging cyber norm to prevent unauthorised modification of information. Integrity also covers trust in the accuracy, completeness and reliability of information.[50]

In this discussion, the focus is on the security aspect of a particular implementation of this principle. The technological integrity principle supports the need for strong security in technology products. It also argues against the creation of hidden functionality or back-door channels in products that would weaken basic security technologies such as encryption, which are also relevant to practices such as whitelisting[51] of cyber threats in cyber protection tools.[52]

In cryptography, the concept of hidden functionality is particularly worrisome as the primary purpose of encryption is to protect the confidentiality and integrity of data. Encryption is the most effective way to achieve data security. In order to read an encrypted file, you must have access to a key or password that enables decryption. Encryption converts electronic data into another form known as cipher text which can then only be deciphered by key holders.[53]

Most organisations today use encryption widely to protect valuable data and communications. Governments rely heavily on encryption to secure strategic communications and protect vital information such as military and diplomatic decision-making. Financial institutions use encryption to ensure the confidentiality and integrity of customer and transaction data.[54] Preserving these technologies is vital. If regulatory measures were created to weaken encryption for legitimate vendors, one must remain mindful that it would do nothing to curb the parallel, 'underground' cryptographic tools developed by malicious users. In essence, the measures would instil a strong sense of insecurity within the legitimate market by sacrificing viable technologies without achieving a meaningful solution for the security issue.[55]

49 For detailed information on the developments in the UN GGE, see chapters 6 and 7.

50 Wamala, International Telecommunication Union, *The ITU National Cybersecurity Strategy*, 13.

51 Whitelisting is the practice by which information, such as credentials, applications and network addresses are added to a list considered trustworthy.

52 Fran Howarth, *Taking Back Control in Today's Complex Threat Landscape …using Application and Change Control to Thwart Attackers: White Paper* (London: Bloor Research, 2011), http://www.mcafee.com/us/resources/white-papers/wp-bloor-application-change-control.pdf.

53 Ahmad Kamal, *The Law of Cyber-Space: An Invitation to the Table of Negotiations* (Geneva: United Nations Institute of Training and Research, 2005), https://www.un.int/kamal/sites/www.un.int/files/The%20Ambassador's%20Club%20at%20the%20United%20Nations/publications/the_law_of_cyber-space.pdf.

54 Mark Hickman, 'Why Financial Institutions Need Data Encryption Education,' *CreditUnionTimes*, October 26, 2014, http://www.cutimes.com/2014/10/26/why-financial-institutions-need-data-encryption-ed.

55 Sara Sorcher, 'Influencers: Stronger Encryption on Consumer Devices Won't Hurt National Security (+Video),' *The Christian Science Monitor*, March 11, 2015, http://m.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0311/Influencers-Stronger-encryption-on-consumer-devices-won-t-hurt-national-security-video.

The weakening of encryption may also mean that some malicious actors would be more likely to exploit the mandated weakness by gaining possession of the master encryption key. Cracking strong encryption is an arduous and resource intensive process. It is therefore not an ideal method for a criminal who wishes to remain swift and undetected, unless it is known that the technology has a built-in vulnerability which streamlines the procedure.[56]

Renowned security expert and cryptographer Bruce Schneier warned that various governments' proposals to ban strong encryption threaten to 'destroy the Internet'.[57] Due to encryption, online banking, e-commerce transactions and exchange of communications can be conducted with security and ease, and there are also less obvious ways in which encryption assists on a daily basis. Schneier observed that, in many nations, it helps dissidents, journalists and human rights workers stay alive, and in an era where widespread computer security is still in its infancy, it is a safeguard measure that works well.[58]

With regard to the installation of backdoors, US FBI Director James Comey has stated:

> '... it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end – all in the name of privacy and network security.'[59]

Contrasting views were expressed by Vice Chairman of the US Joint Chiefs of Staff Admiral James A. Winnefeld who stated that we would all be better off if our networks were secure. An emphasis was placed on having the peace of mind that secure networks bring, which although posing a harder problem for intelligence, remains a far better option than maintaining vulnerable networks which provide an easy route for any potential security agency investigation.[60]

Backdoors can be introduced into software in a number of ways. A well-crafted stealthy backdoor in one module of the software, such as its cryptographic component, could suffice to compromise many other functionalities. Depending on the intended use of the software, backdoors might materialise at different stages. The negative impact of hidden backdoors cannot be overstated from the perspective of the provider of the technology. Not only does it put at risk the economic activity and create legal liabilities, it also threatens corporate image and brand reputation.

56 Abelson, *et al, Keys Under Doormats.*
57 Rob Price, 'Bruce Schneier: David Cameron's Proposed Encryption Ban Would "Destroy the Internet"', *Business Insider*, July 6, 2015, http://www.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7.
58 Ibid.
59 Abelson, *et al, Keys Under Doormats.*
60 Ibid.

5. State Surveillance

Disturbingly, this trend of backdoor channels can lead to civil liberties infringements as some states may identify the mere use of encryption as illicit behaviour. In certain nations, charges against online communities have been laid implying that merely training in communication security was evidence of criminal wrongdoing.[61] States also undermine freedom of expression and privacy when they penalise innocent actors who use and produce tools to facilitate Internet access for citizens. For example, a report by the UN Human Rights Council stated that the rights to 'privacy and freedom of expression are interlinked' and found that encryption and anonymity are protected because of the critical role they can play in securing those rights.[62] Mandated backdoors would needlessly weaken and disrupt technology, undermine both its credibility and its innovation capacities, and provide an ideal environment for malicious actors.

Revelations over state surveillance practices have brought the issue of hidden functionality to the fore. As a result, encryption has become a main topic in the debate over privacy rights.[63] The typical justification behind calls for weakening of Internet technologies is for governments and law enforcement agencies to exercise greater control in tackling cyber crime and terrorism.[64] Both law enforcement and governments have called for access to information,[65] including end-to-end encrypted data, because the mounting use of encryption undermines investigative capabilities. Some proposals have called for communication systems and data storage to be designed to allow for exceptional access. However, this recommendation is unworkable in practice, raises ethical and legal issues, and represents a step backwards in terms of cyber security at a crucial period of time when Internet vulnerabilities are being so thoroughly exploited by criminals.[66]

Granting such exceptional access provisions to governments requires a significant amount of trust that governments will not use the data for untoward purposes and will be able to protect the security of the data itself. Confidential information such as banking and other sensitive proprietary data could be placed at higher risk. There have also been a large number of government data breaches which does not instil confidence that networks and systems are properly protected. Exceptional access provisions in democratic societies would also spur nation states with poor human rights records to do the same.[67]

---

61 United Nations, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, A/HRC/29/32 (22 May 2015), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

62 Ibid.

63 Nicole Perlroth, 'Security Experts Oppose Government Access to Encrypted Communication,' *New York Times*, July 7, 2015, http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html.

64 United Nations, Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (September 2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

65 Abelson*, et al, Keys Under Doormats.*

66 Ibid.

67 Perlroth, 'Security Experts Oppose Government Access to Encrypted Communication.'

From a public policy perspective, the natural answer would be to provide law enforcement personnel with the best possible tools in order to investigate crime, subject to due process. However, on scientific analysis, there is a distinguishing feature present between what may be desirable versus what is technically possible.[68]

Concerns about mass surveillance continue to grow due to the increased investments in offensive cyber capabilities by states that view cyberspace as a new domain of warfare. Revelations continue to emerge that many nations engage in large-scale cyber espionage, leveraging technology tools at their disposal or exerting pressure over technology providers in their jurisdiction. Press reports abound on how government intelligence agencies covertly exploit commercial technologies for cyber espionage, much in the same way as cyber criminals and other malicious players would.[69] Such revelations are often met with either officially issued statements, or claims that the purposes were not malicious or fraudulent, but rather served legitimate public policy objectives such as national security and counterterrorism. Regardless, these scenarios highlight the importance of commercially available technologies such as encryption being secure, uncompromised, and free from backdoors. Robust encryption is still regarded as highly effective for protecting electronic data, including from some surveillance and intelligence agencies who have reportedly tried and failed to circumvent them[70] and should be regarded as one of our most important defences.[71]

Aside from mass surveillance, backdoors may also create an environment of conflict which, if attributed to another state, generates political tension and may lead to retaliatory measures. If political tensions between countries already exist, such actions could lead to escalation. In addition, the erosion of public trust in the underlying technology infrastructure reduces its economic value as a driver of innovation, growth and source of social welfare.

68 Abelson*, et al, Keys Under Doormats.*

69 Jacob Appelbaum, Judith Horchert and Christian Stöcker, 'Shopping for Spy Gear: Catalog Advertises NSA Toolbox,' *Spiegel Online International*, December 29, 2013, www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html; 'Inside TAO: Documents Reveal Top NSA Hacking Unit,' *Spiegel Online International*, December 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

70 Gary McGath, 'Why We Need Encryption Even the NSA Can't Decipher,' *Newsweek*, July 10, 2015, http://www.newsweek.com/why-we-need-encryption-even-nsa-cant-decipher-352073; 'Digital Disease Control. Basic Security Hygiene Goes a Long Way,' *The Economist*, July 12, 2014, http://www.economist.com/news/special-report/21606417-basic-security-hygiene-goes-long-way-digital-disease-control.

71 Rob Price, 'Bruce Schneier: David Cameron's Proposed Encryption Ban Would "Destroy the Internet"'; Alex Comninos and Gareth Seneque, *Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance* (Global Information Society Watch, 2014), https://giswatch.org/en/communications-surveillance/cyber-security-civil-society-and-vulnerability-age-communications-sur.

6. Erosion of Trust in Technology: Economic and Societal Impact

Proponents of technological integrity have stated that introducing hidden functionality into technologies must be opposed as it undermines the entire premise of information and communications technologies. Users of technology need an assurance that products serve the purpose and only the purpose for which they were purchased.[72] Having knowledge (or merely suspicion) that a tool could have backdoors would automatically disqualify the product and its vendors to both the consumer and community at large. This would result in devastating economic consequences for the technology sector and users would also lose the benefit of access to the latest and most innovative technologies.

The economic impact would be twofold. First, the cost of devising and implementing a key escrow[73] system on the scale which would be required by the growing Internet would be exorbitant. Second, it has been calculated that revenues would be lost due to global consumers losing confidence in the security of technology products and services.[74] In the absence of encryption, as well as other protective and security technologies, secure transfer protocols (SSL and TLS) would not exist, leaving countless consumers' personal, health and financial information vulnerable to espionage and theft.[75] It also would further compound the already substantial economic impact of the mass surveillance revelations of recent years.[76]

Trust in technology – or at the very minimum an assurance of trust in technology – is paramount as illustrated by recent occurrences. As has been reported in the media, the existence of a complex environment of many entities (suppliers, system integrators, external service providers, etc.) may have provided an opportunity for supply chain circumvention by intelligence agencies who then reinserted the products back into the market place.[77] Mere speculation of involvement was enough for reputable multinational ICT vendors to be forced to issue broad statements, risking significant erosion of their brand reputation and the business consequences that may attach.[78]

Weakening encryption would undeniably have a profound effect on the economy. In the US alone e-commerce has grown from $100 million total annual sales in 1994

72 Appelbaum, Horchert and Stöcker, 'Shopping for Spy Gear: Catalog Advertises NSA Toolbox.'

73 Key escrow system is a data security measure in which keys required to decrypt data are held in escrow, so that in necessary circumstances an authorized third party may be able to gain access.

74 Ryan Hagemann and Josh Hampson, *Encryption, Trust, and the Online Economy. An Assessment of the Economic Benefits Associated with Encryption* (Niskanen Center, 2015), https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

75 Hagemann and Hampson, *Encryption, Trust, and the Online Economy. An Assessment of the Economic Benefits Associated with Encryption.*

76 Danielle Kehl, 'OTI Policy Director Kevin Bankston Offers Ten Reasons Why Backdoor Mandates Are a Bad Idea: In Testimony before the House Oversight and Government Reform Committee, Bankston Argues against Legislative "Fixes" for Strong Encryption,' *New America*, April 28, 2015, https://www.newamerica.org/new-america/oti-policy-director-kevin-bankston-offers-ten-reasons-why-backdoor-mandates-are-a-bad-idea/.

77 Robert S. Metzger, 'Cybersecurity and Acquisition Practices: New Initiatives to Protect Federal Information of Civilian Agencies,' *Bloomberg Law*, May 20, 2015, http://www.bna.com/cybersecurity-acquisition-practices-n17179926734/.

78 Appelbaum, Horchert and Stöcker, 'Shopping for Spy Gear: Catalog Advertises NSA Toolbox.'

to over $220 billion in 2014.[79] In Europe, e-commerce figures are even higher in the 28 EU member states with total annual sales of €368.8 billion in 2014.[80] Although it is not possible to attribute a precise figure for this growth to the widespread use of secure encryption, it is improbable that such tremendous growth would have taken place without the underpinning trust engendered by security technologies such as encryption and online secure data transfer protocols.[81]

Beyond the strict impact on businesses and the economy, at the societal level, knowledge that governments and other organisations are able to exploit hidden technological capabilities to monitor citizens would consecrate what can only be described as a structural violation of civil liberties, at least in open societies where public oversight over democratically elected governments is the norm. This is of particular concern as public trust in the government's effective use of technology is indispensable.[82]

Furthermore, such measures could lead to criminals and terrorists gaining access to hidden functionality.[83] If the potential targets of surveillance became users of the hidden functionality, the security, stability and welfare of the public could be placed in grave danger. In that sense, the measures proposed to deter terrorism could come at a potentially higher cost to national and economic security, and this crucial point must not be overlooked. The solution cannot be to structurally weaken the protective technology itself.

7. Recommendations

7.1 Developing Specifications for Feasible Requirements

Government and law enforcement demands for exceptional access provisions entail the serious risk that malicious actors (whether individual criminals, terrorists, or nation states) will gain backdoor access to technologies to attack the very population that agencies have a duty to protect. If exceptional access provisions are placed on industry through a transparent process such as legislation, these measures will force industry to make a difficult choice regarding whether or not to comply. For compliance to be possible, authorities will also need to provide evidence of the indispensable need for such drastic measures, outline their requirements, and produce feasible particulars of the specifications for exceptional access mechanisms that

79 Matt Byrom, 'Data Driven Ecommerce – Infographic,' *Business 2 Community*, June 3, 2014, http://www.business2community.com/infographics/data-driven-ecommerce-infographic-0902379#DZoMLO0USQWDOO5G.97.

80 Ecommerce Europe, 'Infographics,' http://www.ecommerce-europe.eu/facts-figures/infographics.

81 Hagemann and Hampson, *Encryption, Trust, and the Online Economy. An Assessment of the Economic Benefits Associated with Encryption*.

82 Gregory T. Nojeim, 'Cybersecurity and Freedom on the Internet,' *Journal of National Security Law & Policy* 4 (2010), http://jnslp.com/wp-content/uploads/2010/08/09_Nojeim.pdf.

83 Comninos and Seneque, *Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance*.

would meet their expectations.[84] In addition, a due process mechanism to secure that access would be required.

Faced with such requirements, industry would need to consider if it is prepared to take the risk of compromising its technology, its brand image, and its duty to its customers with the potential consequence of either departing from a product line or making it unavailable in a particular market. There would be long term consequences other than the loss of economic activity. Experience shows that the prospect of an alternative technological solution that would circumvent local government requirements is very likely.[85]

If a point is reached where technology is effectively compromised, it will not only impact the industry from a business point of view, but it will also mark the end of cyber security as we know it. The result will be that data of governments, businesses and individuals will be in the open and they will be unable to protect themselves using legitimate means. In such a situation, only malicious actors would stand to win, and terrorists, criminals and cyber criminals in particular will find and develop other clandestine and confidential ways to communicate. Or, to put it very simply and quoting the creator of PGP encryption: 'if privacy is outlawed, only outlaws will have privacy'.[86]

7.2 Remaining Open to Alternative Policy Options

Given such compelling arguments against undermining the integrity of security technologies, it may also be worth considering altogether different policies that could achieve the targeting of illegal actors and facilitate the targeted interception of criminal and malevolent communications without compromising the foundations of cyber security and trust in the Internet. Carefully drafted, balanced policy measures could seek to maintain digital traces on the Internet without indulging in mass surveillance, or undermining the integrity of the technology. Advanced and novel investigative tools to collect digital evidence may then be leveraged in a well targeted and narrowly focused manner.[87]

This approach would both increase the legitimacy of the targeted surveillance operations that are necessary in the interest of public security, and create meaningful safeguards against undue, unnecessary or disproportionate practices such as generalised mass surveillance. Discussions in that direction are ongoing in several countries, notably to explore the option of retaining[88] electronic communications data for the purpose of combatting crime and terrorism. Other countries are considering steps associated with the removal of some anonymity associated with some

84 Abelson, *et al, Keys Under Doormats.*

85 'Mass Surveillance Isn't the Answer to Fighting Terrorism,' *New York Times*, November 17, 2015, http://www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html.

86 Philip R. Zimmermann, *Why I Wrote PGP* (Colorado: Boulder, 1991), https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

87 'German Parliament Votes for New Data Retention Law,' *Deutsche Welle*, October 16, 2015, http://www.dw.com/en/german-parliament-votes-for-new-data-retention-law/a-18786345.

88 Electronic Frontier Foundation, 'Mandatory Data Retention,' https://www.eff.org/issues/mandatory-data-retention.

online and communications transactions. For example, Belgium has proposed the requirement for identification documents in order to purchase a SIM card.[89]

7.3 Careful Balancing of Cyber Security and National Security

Despite the fact that nations feel more vulnerable every day as their reliance on cyber infrastructure increases, governments should avoid falling prey to fear mongering and giving in to the introduction of backdoors.[90] A fine line should be drawn between cyber security and national security issues, as a national security slant may lead to greater civil liberty infringements and subsequent loss of technological integrity.[91]

7.4 Increased Public Awareness and Education

At the broadest level of economy and society, emphasis should be placed on public awareness and education campaigns focusing on cyber security measures beginning at home and highlighting the importance of updating software regularly and the use of up-to-date security and privacy enhancing technologies.[92]

7.5 Maintaining Integrity in Technology

For this to work in practice, trust in the integrity of technology will be indispensable. Symantec firmly calls for the recognition of the principle of technological integrity as a critical cyber norm. More than a public policy consideration and recommendation, this is also the value proposition and core principle on which Symantec's business is built. Therefore, as a company, Symantec not only professes technology integrity, but also abides by it. Our corporate principles are clearly spelled out by Executive Vice-President and General Counsel Scott Taylor that Symantec:

- Does not introduce hidden functionality (back doors) in its technologies;
- Does not whitelist malware in its security solutions;
- Does not keep copies of encryption keys that its corporate customers use, and consequently does not have the ability to comply with requests to produce such keys; and
- Uses the highest known standards for encryption and believes that its encryption technology is secure and has not been undermined.[93]

The purpose and role for introducing the principle of technological integrity as a cyber norm is to make a compelling case for a technology provider's right to make

89 'The Economist Explains: How to Improve International Cyber-Security,' *The Economist*, November 29, 2015, http://www.economist.com/blogs/economist-explains/2015/11/economist-explains-20.

90 Kopstein, 'The Feds Don't Need Digital Backdoors – They Can Hack You.'

91 Ron Deibert has made this argument in Ron Deibert, *Distributed Security as a Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* (Calgary: Canadian Defence & Foreign Affairs Institute, 2012), https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf.

92 Comninos and Seneque, *Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance*.

93 Scott Taylor, 'Reaffirming Symantec's Commitment to Security and Privacy for the Online World,' *Symantec Connect*, December 19, 2014, http://www.symantec.com/connect/blogs/reaffirming-symantec-s-commitment-security-and-privacy-online-world.

these claims and abide by them. In addition, the aim is to provide industry operators with an internationally recognised legal basis to oppose government requests and injunctions that would be incompatible with these principles, as well as with due process.

8. Conclusion

The private sector has an important role to play in the development of cyber norms. Despite the fact that cyber norms are, in principle, the result of government-to-government deliberations, the private sector is affected by and influences the development of cyber norms through cooperation and partnership mechanisms. Technological integrity is an emerging cyber norm of growing significance because of the direct link it has with trust in the Internet, technology, market forces, and human rights. The debate on technology integrity is affected by the growing concerns states have about public safety and national security.

The lack of a cyber norm on technological integrity creates an environment in which fundamental rights to privacy are breached, security measures are compromised, and economic growth diminishes. However, as law enforcement and governments become aware of terrorist or criminal plots which are increasingly difficult to detect due to the use of unsuspecting forms of encrypted technology, debates regarding encryption will continue.[94]

Therefore, it is more critical than ever to ensure that policy-makers support the establishment of a cyber norm on technological integrity and achieve consensus around it. They need to be made aware of the inefficiencies and unintended consequences of weakening security technologies such as encryption, and to pursue alternative policies that will enable them to fight crime while protecting human rights, trust and economic growth. Achieving an appropriate balance between cyber security and national security while respecting technological integrity should remain a key public policy objective.

94 Kate Day, 'Why Terrorists Love PlayStation4,' *Politico*, November 25, 2015, http://www.politico.eu/article/why-terrorists-love-playstation-4/; Katrin Bennhold and Michael S. Schmidt, 'Paris Attackers Communicated with ISIS, Officials Say,' *New York Times*, November 15, 2015, https://web.archive.org/web/20151115191248/http:/www.nytimes.com/2015/11/16/world/europe/paris-attackers-communicated-with-isis-officials-say.html; Ellen Nakashima and Greg Miller, 'Why It's Hard to Draw a Line between Snowden and the Paris Attacks. The Debrief: An Occasional Series Offering Reporters' Insights,' *The Washington Post*, November 19, 2015, https://www.washingtonpost.com/world/national-security/why-its-hard-to-draw-a-line-between-snowden-and-the-paris-attacks/2015/11/18/34793ad4-8e28-11e5-baf4-bdf37355da0c_story.html.

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

CHAPTER 11

Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms

Claire Vishik, Mihoko Matsubara, Audrey Plonk

1. Introduction

1.1 Definition of Cyber Security

Cyber security is a complex subject and has a number of definitions, such as this from the National Initiative for Cyber Security Careers and Studies (NICCS):

> 'The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.'[1]

The same source also offers an extended definition:

> 'Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military,

1 NICCS, 'Explore Terms: A Glossary of Common Cybersecurity Terminology,' https://niccs.us-cert.gov/glossary.

and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.'[2]

1.2 Multidisciplinary Context for Cyber Security Norms

In this chapter, we do not attempt to offer a comprehensive analysis of various cyber security contexts, but rather to compare common elements in a set of representative documents and explore the connection between shared principles and domain-specific norms in a context that encompasses policy, technology, and societal issues.

The white paper adopted by several industry associations in Europe, Asia, and the US, entitled *Moving Forward Together: Recommended Industry and Government Approaches to the Continued Growth and Security of Cyberspace,* observes: 'Technology and services change and evolve rapidly, and policymaking related to cyberspace must also be innovative to support growth, security, trust and confidence, and stability'. All stakeholders (government, industry, academia, and civil society) must work together to ensure that the benefits of cyberspace are accessible to citizens, and that major challenges are addressed.[3] While a government is responsible for developing policies, strategies, and regulatory conditions for the development of cyber security, industry is the source of cutting-edge technologies, technical expertise, deployment and operational experience, and, in many countries, owns major components of critical infrastructure. Multi-stakeholder cooperation requires a common context to enable the participants to collaborate constructively. Industry owns and operates a significant part of the Internet infrastructure and develops and deploys technologies responsible for the operations and evolution of cyberspace. For both industry and government, the shared context is important because it permits regulators to design policies consistent with the technology space and flows of information and allows industry to introduce products and solutions that are aligned with high-level principles and based on specific norms and best practices. A richer context proposed in this paper could explain, for example, why an implementation of a network service is compliant with generally accepted privacy requirements, and what best practices and technology norms, such as the use of privacy-preserving cryptographic protocols, have been employed to achieve these goals. In another example, rich context can provide practical guidance on solutions available to increase the reach of cyberspace to areas with limited infrastructure based on the standards and technologies available today. The need for the shared context in cyber security and challenges associated with its creation are also highlighted in research.[4]

2 Ibid.

3 'Moving Forward Together: Recommended Industry and Government Approaches for the Continued Growth and Security of Cyberspace' (*BSA* | The Software Alliance, et al, Seoul Conference on Cyberspace 2013, October 2013), 1-2, http://www.itic.org/dotAsset/9/d/9dede1e6-0281-4c19-84c5-00b8209b7bea.pdf. Adopted by five industry associations in conjunction with the Cyber Space Conference in Seoul in 2013.

4 Jeffrey Hunker, 'Policy Challenges in Building Dependability in Global Infrastructures,' *Computers & Security* 21 (2002): 705-711; Bruce L. Benson, 'The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement without the State,' *Journal of Law, Economics and Policy* 269 (2005).

There are a number of multi-disciplinary principles or guidelines that should be approached as a whole, to ensure that societal, policy, and technology aspects are integrated; this is illustrated in Table 1, which is based on the example offered by OECD Guidelines for cyber security.

Table 1. Nine Principles from the OECD Guidelines.[5]

Type of Elements	Principles	Description
Policy, organisational	Awareness	Needs and requirements for security of information systems and benefits of their implementation should be recognised
	Responsibility	Responsibility for the security of information systems and networks should be shared by all
	Response	Timely and co-operative way to prevent, detect and respond to security incidents is necessary
Technology	Risk assessment	Regular structured risk assessments should be conducted
	Security design and implementation	Security should be incorporated as an essential element of information systems and networks
	Security management	A comprehensive approach to security management should be adopted
	Reassessment	Appropriate modifications to security policies, practices, measures and procedures should be made as the environment changes
Societal	Ethics	Legitimate interests of others should be respected; work should be conducted in an ethical manner
	Democracy	The security of information systems and networks should be compatible with essential values of a democratic society

While the development of high level concepts and guidelines has been relatively successful, it has proved a challenge to define a multi-disciplinary integrated model that could allow technologists and policy-makers to easily collaborate on developing viable cyber security policies and approaches to cyber norms that are compatible with a quickly evolving technology environment. The global nature of the Internet and the ubiquitous use of cyberspace worldwide require the amalgamation of various disciplines and the collaboration of academia, government, industry, and civil society organisations. However, the research and practitioners community has not developed a mechanism to link more concrete and frequently domain-specific norms to the high-level principles in a scientific and predictable fashion.

The lack of a rich common context, comprising both principles and norms, has delayed the emergence of harmonised mechanisms which would enable the multi-stakeholder community to build on the shared values associated with the societal, policy, and technological aspects of cyber security. It has also led to weaknesses in the technology space, where policy requirements are not always adequately incorporated, and in policy design, where technology constraints are not always well understood.

5 'OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security' (Organization for Economic Co-operation and Development, 25 July 2002), 10-12, http://www.oecd.org/sti/ieconomy/15582260.pdf.

1.3 Principles and Norms

As the article focuses on establishing a common context, it is necessary to use broad, all-encompassing definitions. A norm is simply defined as a standard, model or pattern, in reference to technology norms and best practices discussed in this chapter. These norms are based on high-level principles, defined as basic truths, theories or ideas that form a basis of something.[6] This chapter discusses policy principles. Multi-stakeholder groups frequently focus on the development of principles because the high level of generalisation permits diverse participants to form convergent views. Norms, especially technical norms, are more frequently defined by communities with specialised knowledge and expertise. Although efforts are made to design technical norms and best practices based on accepted policy principles, the link between the norms and the principles and between the technology and the policy space is highly abstract. This level of abstraction simplifies consensus, but also complicates discussions on design and implementations of cyber security policies that take into consideration both norms and principles.

The typical (and constructive) approach in multi-stakeholder efforts in cyber security is to propose common high-level policy principles and to ensure that the technical norms are developed in accordance with them. This top-down view leads to positive results for agreeing on industry norms. An example of such consensus achieved on high-level principles in a complicated area is the encryption principles developed by the World Semiconductor Council.[7] However, this approach is not always sufficient for the incorporation of the requirements defined by the technology space and technology constraints into the policy design process. The limitations are due in part to the complexity and dynamism of the technology environment and relative slowness of the policy response. It is not realistic to expect expert knowledge of technology from the policy-makers and an expert knowledge of policy from the technologists. We hope that the ontology proposed here can provide both philosophy and tools for defining a broadly applicable richer shared context that helps multi-stakeholder efforts to agree on the principles and provide operational context for norms.

The absence of mechanisms to transition more objectively from principles to norms hinders the development of common ground in complex and multidisciplinary fields, like cyber security. As an example, support for privacy is a shared principle in most cyber security strategies, but the nature of technical standards, norms, and best practices that are necessary in different technology contexts and the constraints imposed by technologies are not clear to the policy-makers, leading to imperfect regulations that are difficult to harmonise internationally. In other words, recognition of the essential character of privacy in connection with cyber security is not actionable without a predictable linkage to best practices (norms

6 Definition from Merriam-Webster, 'Principle,' http://www.merriam-webster.com/dictionary/principle.

7 'WSC Encryption Principles' (World Semiconductor Council, Lisbon, 23 May 2013), http://www.semiconductors.org/clientuploads/Trade%20and%20IP/May%202013%20WSC%20-%20WSC%20Encryption%20Principles-%20FINAL.pdf.

and standards), such as data anonymisation techniques or obfuscation of unique identifiers. In a different example, understanding of technology constraints, such as the impossibility of complete anonymity in today's computing environment, is necessary in order to create regulations and policies that are effective, such as guidelines for data protection. The introduction of a scientific reasoning process based on ontology that links policy principles and technical best practices would improve regulatory design and extend opportunities for self-regulation. Predictability would also increase trust in industry norms and best practices through the recognition of their connection to generally accepted principles in situations ranging from policy implementation to support for self-regulation.

The level of complexity of multi-disciplinary issues in cyber security also requires decision and dialogue support tools, and an ontology linking principles and norms can provide a foundation for such a mechanism.

1.4 Ontology as a Consensus-Building Tool

Ontology in computer science can be defined as 'a formal naming and definition of the types, properties, and interrelationships of the entities that really or fundamentally exist for a particular domain of discourse'.[8] Ontology permits us to highlight connections and relationships between terms, identify constraints, and to reason about a topic. Ontologies are commonly used in a variety of settings in cyber security, such as creating threat and vulnerability models for innovative fields.

Ontologies enable a structured organisation of knowledge and creation of a multifaceted context with reasoning capabilities. The complexity of the field of cyber security and the need to formulate relatively simple technical norms and best practices that are connected to general policy principles point to ontology as the tool of choice to capture relationships between concepts, principles, and their attributes and to enable robust modelling of constraints and complex situations.

While ontologies have been used in a number of fields, from e-commerce to enterprise systems, they have not yet been employed as a 'dialogue support' mechanism for multi-stakeholder initiatives in complex fields. For examples of ontologies used in knowledge engineering of diverse domains, repositories such as the Protégé Ontology Library[9] are recommended. Ontologies for cyberspace have also been created by, for example, Kopsell.[10] The introduction of a well-designed ontology could help the participants to create a framework for reasoning about cyber security norms in connection to shared principles, and to understand the mutual connections of the best practices, thus improving the efficiency of outcomes. The benefits will be significant for policy-makers and policy theorists, allowing them to improve their understanding of the complex technology space, and for industry, to support design and positioning of norms and best practices in a correct policy context.

8 See, for example, Wikipedia, 'Ontology (Information Science)', https://en.wikipedia.org/wiki/Ontology_(information_science).
9 Protégé Ontology Library, 'OWL Ontologies,' http://protegewiki.stanford.edu/wiki/Protege_Ontology_Library.
10 David R. Koepsell, *The Ontology of Cyberspace: Law, Philosophy, and the Future of Intellectual Property*, (Peru, Illinois: Open Court Publishing, 2000).

Although we do not propose a concrete design for a 'multi-stakeholder dialogue support' ontology in this paper, we can identify foundations, upon which it can be built:

- *High level policy principles (top layer)* can be derived from commonly accepted key concepts identified by earlier efforts. This chapter is primarily focusing on this area.
- *Technology characteristics* can be established based on the accepted attributes of the technology environment and input from various experimental frameworks developed to analyse it.
- *Norms, standards and best practices* can be developed by the communities of experts and incorporated into the ontology.

The resulting ontology can arm multi-disciplinary initiatives with the ability to conduct in-depth conversations that rely on consistent background knowledge and do not over-simplify key issues, leading to better results. As an example, the Public Initiative on Cyber-Physical Systems (CPS) convened by NIST[11] proposed a risk-based framework for CPS that links risk domains of privacy, security, safety, resilience, and reliability in one integrated model. The insights resulting from this work can inform regulation and standardisation for the Internet of Things (IoT). The integrated risk model represents a set of general principles that can be used to analyse risk for the IoT. The reference framework produced by the same public working group extracts concrete elements that can make future IoT systems trustworthy. An ontology can link the high-level risk principles and concrete technical norms in this and similar initiatives, in order to permit technologists and regulators to jointly reason about optimal technology environments and the policy approaches that govern them.

Although a consistent shared context has not yet been generally adopted, even at the level of principles, some fundamental concepts have been defined as part of a number of industry- or government-led efforts. Incorporation of these elements of shared vision could speed up the creation of the body of knowledge to support consensus-building on major issues in cyber security. The section below describes these common elements as a potential foundation of a future shared context in an ontology to be used in multi-stakeholder initiatives. We start the discussion with the analysis of the most pertinent characteristics of the technology environment since they provide additional linkage between high level principles and norms.

11 Cyber-Physical Systems Public Working Group, http://www.cpspwg.org/.

2. Technology Environment

Today's dynamic technology environment supports seamless functioning of all societies around the globe. This section attempts to extract key characteristics of the technology environment that are also pertinent to policy-making in cyber security. We describe key characteristics that have been commonly recognised and that are broadly applicable. Broad categorisation of these attributes is illustrated in Table 2 below, and they form a foundation for technology principles to be used in the ontology we are describing.

Table 2. Key characteristics of the technology space by broad category.

Category	Attribute
Technology	Universal Connectivity
	Complexity and dynamic nature
	Influence on the physical environment
	Shared nature of infrastructure
Societal	Global and universal use of cyberspace
	Broad economic impact of cyberspace

2.1 Ubiquitous Connectivity and Interoperability

The modern computing environment is characterised by ubiquitous connectivity and interoperability between heterogeneous networks and diverse systems and devices. The numbers of connected devices cannot be estimated with great precision, but is extremely large. EMC Corporation estimates over 7 billion people will use 30 billion Internet-connected devices by 2020,[12] whereas Cisco and DHL predict a higher number – 50 billion connected devices by the same date.[13] Disparate computing and network domains of fifteen years ago have merged into an interconnected space that supports multiple models of use, connectivity, and access via shared infrastructure. The diversity of connected devices is enormous, including everything from data centres and full PC platforms to tablets, industrial control systems, disposable sensors and RFID tags, and it is matched by the diversity of the networks. Ubiquitous connectivity is beneficial for the users of the technologies and for the economy, leading to new efficiencies and increased productivity, and providing a platform for widespread innovation. The challenges created by this environment are well known. Universal connectivity and interoperability complicate the analysis of threats and vulnerabilities, lead to uneven levels of protection in interconnected systems and elements of infrastructure, and, in many cases, can increase attack surfaces.

Ubiquitous connectivity and broad interoperability support movements of data

12 EMC^2, *New EMC Innovations Redefine IT Performance and Efficiency*, 4 May 2015, http://www.emc.com/about/news/press/2015/20150504-01.htm.

13 Cisco, 'Internet of Things (IoT),' http://www.cisco.com/web/solutions/trends/iot/portfolio.html.

over diverse networks and are important for numerous areas of policy-making, including standards policies, network and information security regulations, and data protection. Policy developments that hinder the open nature of the Internet, such as data localisation or reliance on indigenous standards, can become obstacles to global interoperability and inhibit the role of cyberspace as a powerful engine of economic growth.

2.2 Intrinsic Complexity and Dynamism of the Technology Environment

Interoperable frameworks that form the foundation of the modern technology environment are likely to contain unknown vulnerabilities due to the effects of composition of diverse security models.

We have not yet developed mechanisms to analyse the composite picture of infrastructure that is today's reality. Complexity is obvious in the multi-domain processes typical of today, as there are a number of technical domains employed to achieve one operation. Although the process is designed to reach one operational goal, their security capabilities are different at different stages of the process. Defining 'trust evidence' for this environment has proved very challenging.[14]

With no objective approaches to estimating the security of complex systems under operational conditions and no standards to apply to diverse environments where they operate, it is difficult to comprehend the consequences of system level or environmental changes. This complexity and ambiguity also applies to data and data protection, making it necessary to re-think a number of fundamental concepts such as anonymity and data interoperability.

Complexity of the computing environment is the result of the aggregation of various frameworks and underlying security and privacy models that were designed in isolation. The impact of complexity needs to be well understood in order to correctly inform the development of effective cyber policies. Policy-makers frequently examine cyber security concerns at a simplified level, making generalisations that become disconnected from the evolving capabilities of the complex technology space. These policies need to be technology-neutral,[15] but also aware of the key characteristics of the technology space in order to incorporate the crucial relationships between norms and best practices in cyber security.

2.3 Intermingling of Cyber and Physical Components

Another important characteristic of cyberspace is the connection between cyber and physical environments, as exemplified in Cyber-Physical Systems (CPS), systems of systems that have computing components, communication capabilities, and

14 Claire Vishik, Anand Rajan, Chris Ramming, David Grawrock, and Jesse Walker, 'Defining trust evidence: research directions,' *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '11)*, Frederick T. Sheldon, Robert Abercrombie, and Axel Krings, eds. (ACM: New York).

15 Technological Neutrality is 'the freedom of individuals and organizations to choose the most appropriate and suitable technology to their needs and requirements for development, acquisition, use or commercialisation, without dependencies on knowledge involved as information or data': Wikia, 'Technology Neutrality,' http://itlaw.wikia.com/wiki/Technology_neutrality.

physical subsystems.[16] CPS, now ubiquitous, requires more complex and integrated security and risk models. For CPS, the traditionally separated domains of safety, resilience, reliability, security, and privacy, are intertwined.[17] Separate assessment of these domains is insufficient to address the risks, because requirements optimised for one domain can be detrimental to the composite risk picture of a system or an area of infrastructure. Characteristics of CPS such as the presence of a physical subsystem and real-time controls may demand a departure from traditional views on security or privacy requirements and instead put an emphasis on safety and reliability, such as when developing risk models for nuclear power station management, where privacy concerns are minimal while safety and reliability requirements are crucial.

Stuxnet is an example of an attack carried through cyber-physical environments[18] that illustrates the need to analyse the requirements for all relevant risk domains using an integrated process. Only collaboration between multidisciplinary policy and technology teams can help address these risks. Tools supporting aggregation of different fields, such as the proposed ontology, can help in developing complex norms that span several risk domains, like privacy, cyber security, safety, and reliability.

2.4 Shared Global Infrastructure Based on Open Standards

The benefits of the shared global infrastructure and open standards are clear to all. We can use the same devices, applications, networks, and processes in France and Japan, China and Egypt; for the most part, technology now speaks a common language.

The consensus on the importance of the global shared infrastructure and open standards predates the commercial Internet, but concerns about its dependability emerged early in the Internet history and crystallised into a separate area of research in the mid-1990s.[19] Strong focus on the protection of critical infrastructure has led some researchers such as Dunn Cavelty to assert that 'militarisation of cyber security' was under way.[20]

The infrastructure is shared among the different users of cyberspace from education to transportation and energy, and by different geographic regions underlying the functionality of generic systems and processes. Uneven availability of expertise and resources has resulted in varying levels of cyber security and privacy protections in the infrastructure, stressing the need for policy-makers and technologists to continue to focus on capacity-building in cyber security.

16 See for example definitions at the Cyber-Physical Systems Public Working Group.

17 See deliverables of the NIST from Cyber-Physical Systems Public Working Group.

18 [Stuxnet] 'was a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant. … The key compromise was that Stuxnet placed itself in a critical path where it could not only disrupt the plant process, but also disrupt/manipulate the information flow to the system operator. In this particular instance of Stuxnet, it caused the fast-spinning centrifuges to tear themselves apart, while fabricating monitoring signals to the human operators at the plant to indicate processes were functioning normally.': David Kushner, 'The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program,' *IEEE Spectrum. IEEE*, February 26, 2013, 49-53. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet#.

19 Jeffrey Hunker, 'Policy Challenges in Building Dependability in Global Infrastructures.'

20 Myriam Dunn Cavelty, 'The Militarisation of Cyber Security as a Source of Global Tension,' in *Strategic Trends* 2012, ed. Daniel Möckli (Zurich: Center for Security Studies, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2007043.

2.5 Global Use of Cyberspace and Its Significant Impact on the Economy

Around 40% of the world's population used the Internet in 2014.[21] Twenty years ago, in 1995, the level of connectivity stood at 1% of the population. The number of Internet users grew at 7.9% in 2014, more than seven times faster than the population growth of 1.14%. Some 78% of the populations of developed countries and 31% of those of the developing world were connected in 2014.[22] With such a large population of users, cyberspace-dependent processes permeate the fabric of everyday life. The global nature and scope of cyberspace require strong understanding of the complex underlying technologies and patterns of use as well as policy frameworks enabling cyberspace use. Norms and best practices created in this context need to be actionable and broadly applicable.

The ICT sector has a significant impact on the global economy. By 2010, it represented 6% of global GDP and accounted for 20% of employment in OECD countries.[23] The sector is responsible for increasing productivity and improving efficiency in other sectors, and its impact on all aspects of everyday life and commerce is enormous. Although the development of the technology is rapid, the process of building a unified economic theory for cyber security and providing recommendation on optimal economic models to achieve improved security coverage has been slow.[24]

The digital economy magnifies the efficiencies achieved by monetary economies and creates economies of scale and scope via intermediation and aggregation of resources. Novel use models emerge and quickly become mainstream, providing a constant source of innovation and alleviating information asymmetry, as illustrated by Akelof's model.[25] Despite the rapid pace of change, there is limited theoretical work to address key economic issues, such as design of viable economic incentives for the development of secure infrastructure.[26] Slow development of the economic theory for cyber security is an inhibitor for the design, implementation, and harmonisation of broadly applicable policies, metrics and the model necessary for building and evaluating cyber security norms.

21 Statistics from Internet Live Stats, 'Internet Users,' http://www.internetlivestats.com/internet-users/.

22 International Telecommunications Union (ITU) estimate: Wikipedia, 'Global Internet Usage,' https://en.wikipedia.org/wiki/Global_Internet_usage.

23 'Moving Forward Together: Recommended Industry.'

24 Johannes M. Bauer and Michel J. G. Van Eeten, 'Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options,' *Telecommunications Policy* 33 (2009): 706-719; and Eric Luiijf, et al, 'Ten National Cyber Security Strategies: A Comparison,' in *Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers*, ed. Sandro Bologna et al. (Springer-Verlag Berlin Heidelberg, 2013), 1-17.

25 George A. Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism,' The Quarterly Journal of Economics 84 (1970): 488-500.

26 Claire Vishik, Frederick Sheldon and David Ott, 'Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment,' in *ISSE 2013 Securing Electronic Business Processes*, eds. Helmut Reimer, Norbert Pohlmann and Wolfgang Schneider (Springer Vieweg, 2013), 133-147.

3. Extracting High Level Concepts for the Ontology

Section 2 explored fundamental technology characteristics of cyberspace. The goal of section 3 is to extract high-level common elements from diverse sources that address both policy and technology aspects of cyberspace and that can be used to populate top levels of the proposed ontology. With no accepted framework in place for the co-development and analysis of technology and policy approaches for cyber security, we find useful input in related research, policy analysis, and industry papers. These common elements reflect shared interests and concerns among industry and government, and thus should form a foundation for an ontology supporting multi-disciplinary work on cyber security policy approaches and norms, by allowing industry to design best practices (technical and process norms) consistent with the accepted high level principles, and by enabling the policy community to understand the connection between the principles and best practices guiding their concrete implementation. It is not a comprehensive list of sources and key concepts, but it is representative, and the sources that we evaluated produced overlapping sets of high-level concepts, suggesting shared views on many aspects in cyber security.

3.1 Theoretical Research Frameworks

A number of technology and policy frameworks have been proposed to enable or facilitate the examination of multidisciplinary subjects in security and privacy. A good example is Technology Dialectics,[27] a model developed by Professor Sweeney to mitigate conflicts between requirements of technology and context of use in society. The goal is to detect potential social and adoption issues early in the technology cycle and resolve them by creating tools to determine whether a technology is demonstrably appropriate for a certain society or context. Although the framework focuses on privacy, it can be used for broader analysis and easily applied to cyber security.

Similar single-domain technology and policy frameworks have been proposed by various researchers, including Golubchikov and Deda for the study of low-energy housing,[28] and Ananda, Pandy, and Punia for the analysis of the power sector in India.[29] The shared elements found in this work are summarised in Table 3 below.

27 Latanya Sweeney, 'Technology Dialectics: Constructing Provably Appropriate Technology,' *Data Privacy Lab* (2006), http://dataprivacylab.org/dataprivacy/projects/dialectics/index.html.

28 Oleg Golubchikov and Paola Deda, 'Governance, Technology, and Equity: An Integrated Policy Framework for Energy Efficient Housing,' *Energy Policy* 41 (2012): 733-741.

29 V. Ananda Kumar, Krishan K. Pandey and Devendra Kumar Punia, 'Cyber Security Threats in the Power Sector: Need for a Domain Specific Regulatory Framework in India,' *Energy Policy* 65 (2014): 126-133.

Table 3. Relevant components of technology/policy frameworks.

Category	Key concepts
Technology	Broad applicability
	Rapid innovation
	Shared infrastructure and context requirements
	Diverse operational models
Societal	Evolving use models and context
	Complex requirements for adoption
	Economic considerations
	Connection to fundamental rights (e.g., privacy)
Approach	Actionable (rather than observational)
	Capable of evolution
	Provably effective

The characteristics found in the technology and policy frameworks that we examined are consistent with those we discussed in section 2. These concepts are useful to inform ontology development, and they point to ontologies as support tools linking technology and societal issues. Similar frameworks are frequently employed to support technology development processes in industry.

3.2 Cyber Security Strategies

Another source of shared high-level concepts is found in cyber security strategies formulated by different countries. The OECD's report, *Cyber Security Policy-Making at a Turning Point: Analysing a New Generation of National Cyber Security Strategies for the Internet Economy and Non-governmental Perspectives on a New Generation of National Cyber Security Strategies: Contributions from BIAC, CSISAC and ITAC*, reveals that cyber security strategies developed by different nations share a number of common elements. Shared approaches include the stated need for enhanced internal operational coordination; reliance on private-public partnerships, interest in improved international coordination, the need to protect fundamental values in cyberspace,[30] as well as reliance on flexible policies for cyber security, supporting the economic development associated with the ICT sector, and engagement in multi-stakeholder dialogue. Other researchers such as Kshetri and Murugesan, who compared the US and EU cyber security strategies,[31] and Luiijf, who examined ten cyber security strategies, highlight similar elements of shared cyber security vision. Common elements of cyber security strategies are summarised in Table 4.[32]

Private ownership and operation of critical infrastructure mean that all the stakeholders (government, academia, industry, and non-profits) need to collaborate

30 'Cybersecurity Policy-Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy and Non-Governmental Perspectives on a New Generation of National Cybersecurity Strategies: Contributions from BIAC, CSISAC and ITAC' (Organization for Economic Co-operation and Development, 16 November 2012), 9, http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

31 Nir Kshetri and San Murugesan, 'EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers,' *Computer* 46 (2013): 84-88.

32 Luiijf, et al, 'Ten National Cyber Security Strategies: A Comparison,' 1-17.

on cyber security issues in order to mitigate cyber threats and enhance resiliency and security while maintaining the interoperability and open Internet.[33] But diverse stakeholders cannot acquire expertise in all the relevant topics. Arming multi-stakeholder initiatives with tools such as a comprehensive ontology, in addition to the typical high level deliverables of multi-stakeholder dialogue, e.g., position papers, can bring more efficiency to the process, allowing industry to elucidate the viability of norms and best practices in a broader context that is easier to understand.

Table 4. Common elements shared by cyber security strategies based on OECD[34] report and other analyses.

Type of Elements	Common Elements	Description
Societal/economic	Economic impact	Quantification of economic benefits of cyber security into the strategy
Organisational/policy	Enhanced government cooperation	Better policy level and operational coordination among multiple agencies
	Public-private cooperation	Engagement of all stakeholders (government, industry, non-profits) in policy and solutions development
	International cooperation	Collaboration with other countries on a range of cyber security issues
	Division of responsibility among various government organisations and sovereignty	Operational role of agencies responsible for national security
	Support for fundamental values	Recognition of fundamental values, such as freedom of expression, privacy protection and the free flow of information as essential
Technology-related	Innovation	Preservation of open Internet as a platform for innovation and economic growth
	Comprehensive coverage	Strategies address the full range of ICT components

3.3 Industry-Led Initiatives

Another source of high-level concepts is furnished by documents created by industry and industry associations. The white paper prepared by five industry associations for Cyber Seoul 2013 provides useful categorisation of areas of focus: economic considerations, social and cultural benefits, cyber security proper, international security, cyber crime, and capacity-building as summarised in Table 5.[35] The paper, which is based on a number of earlier sources, indicates high-level areas which are important for industry and to which more specific norms need to be anchored.

33 'Cybersecurity Policy-Making at a Turning Point,' 10-15.

34 Eric Luiijf, Kim Besseling and Patrick de Graaf, 'Nineteen National Cyber Security Strategies,' *International Journal of Critical Infrastructure Protection* 9 (2013): 7-26; 'An Evaluation Framework for National Cyber Security Strategies' (European Union Agency for Network and Information Security, 11 November 2014), 30-31, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies; 'Cybersecurity Policy-Making at a Turning Point,' 9, 24-52.

35 'Moving Forward Together: Recommended Industry.'

Table 5. High-level categories from Seoul industry paper (2013).

Type of Elements	Key Area	Description
Economic	Economic growth and development	Economic growth is the key contribution of the ICT sector
Policy (legal, organisational)	Development of legal frameworks	Criminal statutes to clarify and enhance law enforcement's ability to prosecute bad actors, to combat cyber crime and enhance international cooperation are available
	International cooperation	Cooperation to advance social, economic, and cultural goals, given cyberspace offers a unique global commons
	Capacity-building	Cooperation to develop additional capabilities in legal, policy, and technology areas
	Response to cyber threats	Cooperation to prevent, detect, and respond to cyber security threats.
	Response to cyber crimes	Work to deter cyber threats, implement tools to identify criminal activities, and carry out coordinated action
Societal	Societal and cultural benefits	Increased access to education, influence on the political process, and support for human rights

The paper illustrates a significant level of convergence on high-level principles between the industry and governments that participated in the Seoul Conference on Cyberspace 2013, based, for example, on the similarities between these approaches and the approaches reflected in cyber security strategies produced by various governments, as described above. An ontology linking these key concepts and more concrete best practices could enable diverse communities to collaborate in greater depth and develop more actionable norms and policies.

3.4 Global Digital Infrastructure Work

Industry, academia and government have developed a number of position papers that provide insights into novel policy approaches that support key trends in technology evolution. Among these documents, Intel's *Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy*[36] explains the foundational nature and importance of Global Digital Infrastructure (GDI) and the need to develop policies that support GDI-based innovation and preserve the users' trust in the digital economy. These policies should support the environment that ensured the success of GDI; openness, interoperability, and economic growth potential and should be technology neutral, based on open standards, fostering international cooperation and strong accountability. The underlying concept is 'the triangle of trust' – a collaboration of industry, government, and NGOs on broadly applicable policy principles, including self-regulation and consumer awareness and education.

Other recent research efforts have studied other aspects of GDI, describing GDI evolution and associated metrics.[37] Max Craglia (2015), editor of the joint project of

36 John Miller and David Hoffman, 'Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy,' *Intel Corporation* (2010), http://blogs.intel.com/wp-content/mt-content/com/policy/Global%20Digital%20Infrastructure%20Policy%20Merged.FINAL.PDF.

37 Ola Henfridsson and Bendik Bygstad, 'The Generative Mechanisms of Digital Infrastructure Evolution,' *MIS Quarterly,* 2013, (37: 3), 896-931.

the Chinese Academy of Sciences and the European Commission on Digital Earth 2020, stressed the importance of incorporating policy constraints when developing specific technologies, in order to avoid complications and speed up adoption, echoing the main thrust of the Technology Dialectics framework.

Table 6. GDI and GDI policy: principles.

Type	Broadly applicable principle	Description
Technology	Interoperability	Seamless interoperation among the components of infrastructure and ecosystem
	Openness	Free flow of data across borders and global access to and sharing of innovation
	Foundation in open standards	Support for innovation, collaboration, and openness without relying on particular technologies
	Dynamic nature and rapid evolution	Quick pace of innovation affecting technology and use models
Societal	Economic growth potential	Strong economic growth with cross-sectoral collaboration
Policy	Self-regulation	Self-imposed rules based on based practices and optimal technology outcomes
	Multi-stakeholder international cooperation	Cooperation across borders and sectors to promote continued innovations, economic growth and trust
	Accountability	Obligation/willingness to take responsibility for performance based on agreed-upon expectations

The high-level common elements and principles discussed in this section form an overlapping representative list drawing from diverse sources produced by industry, government, academia, and non-profits. These concepts and the relationships between them can be used to populate the top level of the ontology we are proposing to support multi-stakeholder work in cyber security.

4. Major Gaps That We Need to Address

In order to create a viable common context for the diverse stakeholders in cyber security, additional research, analysis, and industry assessment efforts are needed. Section 4 identifies some of the more important gaps that need to be addressed.

4.1 Scientific Foundations for Cyber Security

The last decade saw several efforts to move cyber security from a practical discipline to a more theoretical level; to develop a 'science of cyber security' that could provide a common foundation for the increasingly diverse range of cyber security topics. The Federation of American Scientists (FAS) described the issue as follows:

> 'The challenge in defining a science of cyber-security derives from the peculiar aspects of the field. The 'universe' of cyber-security is an artificially constructed environment that is only weakly tied to the physical universe. … Cyber-security requires understanding of computer science concepts, but also shares aspects of sciences such as epidemiology, economics, and clinical medicine; all these analogies are helpful in providing research directions.'[38]

The report concludes:

> 'There is a science of cyber-security. Because it is a science with adversaries, it uses, and will use, many different tools and methods. For the future, as far as can be discerned, there will be new attacks on old technologies, and new technologies that need to be defended.'[39]

Cyber security is a science with mature subfields, but lacking accepted definitions of fundamental concepts such as security composition, assurance, accountability, or trust. Strong and generally accepted scientific foundations for cyber security will be instrumental in developing approaches to policy design and norm development based on shared principles already defined by earlier efforts. We hope that an ontology that we are describing here can be instrumental in unifying definitions and methodologies in different areas of cyber security, in addition to linking technical norms with policy principles.

4.2 Standardisation Strategy, Process, and Policy

Open standards enable the foundation of today's digital infrastructure and are crucial for the seamless operation of cyberspace. Active work on the development of international standards is conducted in a variety of settings, from international (for example, ISO, IEC, and ITU)[40] and national standards bodies (ANSI, BSI, or DIN)[41] to industry standards consortia (IEEE or TCG)[42]. It is recognised that most general-purpose technology and governance standards and specifications have to address security and, in many cases, privacy in order to be viable. The inventory of potentially relevant standards existing today is enormous. There are solid internationally recognised policy mechanisms set up to support the use of open standards, including agreement within the World Trade Organization. Standards are necessary to enable the foundations of the dynamic and open cyberspace.

However, in the area of cyber security, there is a lingering perception that, in order to strengthen national security, open international standards should not be

38 Jason, The MITRE Corporation, *Science of Cyber-Security*, JSR-10-102 (19 November 2010), 1, http://fas.org/irp/agency/dod/jason/cyber.pdf.

39 Ibid, 77.

40 IEC (International Electro-technical Commission), ISO (International Organization for Standardisation), ITU (International Telecommunication Union).

41 *American National Standards Institute (ANSI),* British Standards Institution (BSI), Deutsches Institut für Normung e.V. (German Institute for Standardisation) (DIN).

42 The Institute of Electrical and Electronics Engineers (IEEE), Trusted Computing Group (TCG).

used, even in general-purpose technology environments, and that local or regional standards provide greater security because knowledge about them is more limited. These misconceptions have been disproved by extensive research, and continued development of indigenous standards represents a potential threat to the global nature of the Internet and may exclude some constituencies from using the latest most robust security technologies. Among the areas in standardisation that require further development, the following gaps stand out:

- The dearth of global cyber security standards strategy that can address current priorities, e.g., in the infrastructure area;
- The absence of faster and more efficient processes and greater directional flexibility in standardisation, to match the dynamic nature of today's technology environments;
- A lack of methodologies to address harmonisation of standards policy in different countries and regions; and
- No mechanisms to incorporate regional requirements without jeopardising the global nature of the cyber security standards.

The gaps in the standardisation approaches stem from structural issues, which have led to fragmentation of efforts to develop standards. Many organisations, regionally and internationally, have engaged in developing standards for the same or similar spaces. Examples include international (ISO/IEC) and Chinese standards for a Trusted Platform Module; differing regional approaches to Internet governance and numerous overlapping efforts focusing on IoT standardisation in such organisations as IEEE, ISO/IEC, or ETSI. An ontology that is proposed here can have a unifying influence on both technical and governance standards, allowing the stakeholders to address cross-cutting issues in standardisation for cyber security instead of treating these issues in isolation for each context.

4.3 Absence of a Common Vocabulary and Reasoning Framework

The dynamic evolution of cyberspace and its global nature require multidisciplinary study in a process that can support ideation, harmonisation, deployment, adoption, and maintenance of cyber security technologies and policies in a multi-stakeholder setting.

Policy and technology communities, government, and industry use different paradigms to address shared concerns. Cultural gaps can result from different backgrounds, traditions, and different operational contexts. National security communities, energy and finance sectors, high-tech industry, and other key players use different frameworks to address similar security issues. While policy researchers and policy-makers look at the cyber security landscape from a strategic perspective based on general philosophy of the subject, engineers tend to focus on technology considerations and are frequently unaware of the impact national or international regulations and geopolitical concerns could have on their work. Technologists have

different work cycles and objectives, and use different language to policy researchers and policy-makers to describe similar issues.

In order to overcome cultural and knowledge gaps between policy researchers, regulators and the technical community, a common framework and common vocabulary need to be developed. The lack of this shared context is a major stumbling block leading to the fragmentation of the work of different communities of research and practice. An ontology can furnish reasoning and analysis capability in addition to a common vocabulary, providing a mechanism to overcome cultural differences.

5. Towards a Shared Context: Connecting Principles and Norms

Analysis of literature on different aspects of cyber security furnished us with a list of multi-disciplinary fundamental concepts and principles for the integrated analysis of cyber security issues. These elements could serve as a foundation for an ontology to support more efficient multi-stakeholder dialogues in policy, technology, standardisation, and other areas, and for studying cyber security as a multi-disciplinary scientific subject, incorporating societal, technology, and policy contexts.

The lack of a provable ontology-based connection between high level principles and recommendations, technical feasibility of proposals, pace of innovation, efficiency, and enforceability plays a role in complicating negotiations on complex issues, such as the new Data Protection and Network and Information Security regulations in the European Union. The complexity of the issues requires unrealistic knowledge of the broader context from all the participants. Availability of a broadly applicable 'dialogue ontology' would allow industry to demonstrate how technical norms and best practices support high-level principles and recommendations. Such tools would also help illustrate technology constraints in proposed approaches and find remedies to eliminate contradictions. An ontology would help reduce ambiguity by establishing definitions and relationships between concepts and permitting the stakeholders to reason about consequences of the proposed regulations or the requirements of the current technology solutions and processes, such as international data flows. Most importantly, an ontology linking high-level principles and concrete technical or process norms and best practices would be instrumental in outlining a clearer direction towards the implementation of accepted policy proposals. It would permit the participants to speak the same language, to use the same decision support tools, and to define problems and solutions in the same or similar terms without acquiring comprehensive knowledge of issues.

The use of key concepts as the highest level of the ontology can speed up its development and shorten the discussions associated with the structure of the ontology. An ontology will help avoid over-simplification of cyber security principles and provide a framework to incorporate norms and best practices, linked with the principles in a predictable fashion.

In order to create the common context for in-depth reasoning in support multi-stakeholder discussions, we need to link abstract ideas and concrete actionable concepts, account for dynamisms and rapid evolution of cyberspace, address governments' concerns and users' requirements, and understand the implications created by the technology space. We need to be able to make sense of regional differences and complex patterns of adoption, understand limitations of current approaches, and be able to model radically new solutions.

From the technology point of view, cyberspace is rooted in shared global digital infrastructure (GDI) and includes a variety of technology domains that can form a large number of dynamic contexts. Among these contexts, we can identify smart grid, connected transportation and energy, online education, social networks, organisational and government environment, as well as broader foundations of these contexts, such as 'cloud' or the 'Internet of things'. The environment comprises multiple interconnected technology components such as networks, devices, and data, and also possesses user interfaces and, in some case, physical subsystems.

The technology space has a number of important characteristics that have strong impact on the development of policies and technical norms. They include intrinsic complexity, interoperability, ubiquitous connectivity, and intermingling of diverse contexts, such as cyber and physical. These characteristics need to be taken into consideration in every policy and technology strategy initiative. Over-simplification of cyberspace, while helpful in some contexts, is a poor initial premise for a policy discussion and limits the necessary assessment of constraints and interdependencies impacting the effectiveness of an approach, a legal framework, or a regulation.

The technology space brings significant societal benefits, but its continued success depends on the acceptance of innovation by the society. It has been an economic driver and engine of innovation since its emergence, and has acquired an enormous user base, with 40% of the global population connected, providing access to education, information, and entertainment, supporting consumer and work environments, and underlying every element of critical infrastructure. The consequences of even a small failure of this system of systems are hard to quantify.

The technology environment is based on fundamental characteristics linking the technology environment with the policy space and providing a foundation for the development of industry norms and best practices for cyberspace. Because of the complexity of the environment, cyber security risks are multi-faceted, comprising the adjacent domains of security, privacy, safety, reliability, and resilience. These risk domains can be addressed through private-public collaboration, international cooperation, national coordination, and multi-stakeholder efforts, the key

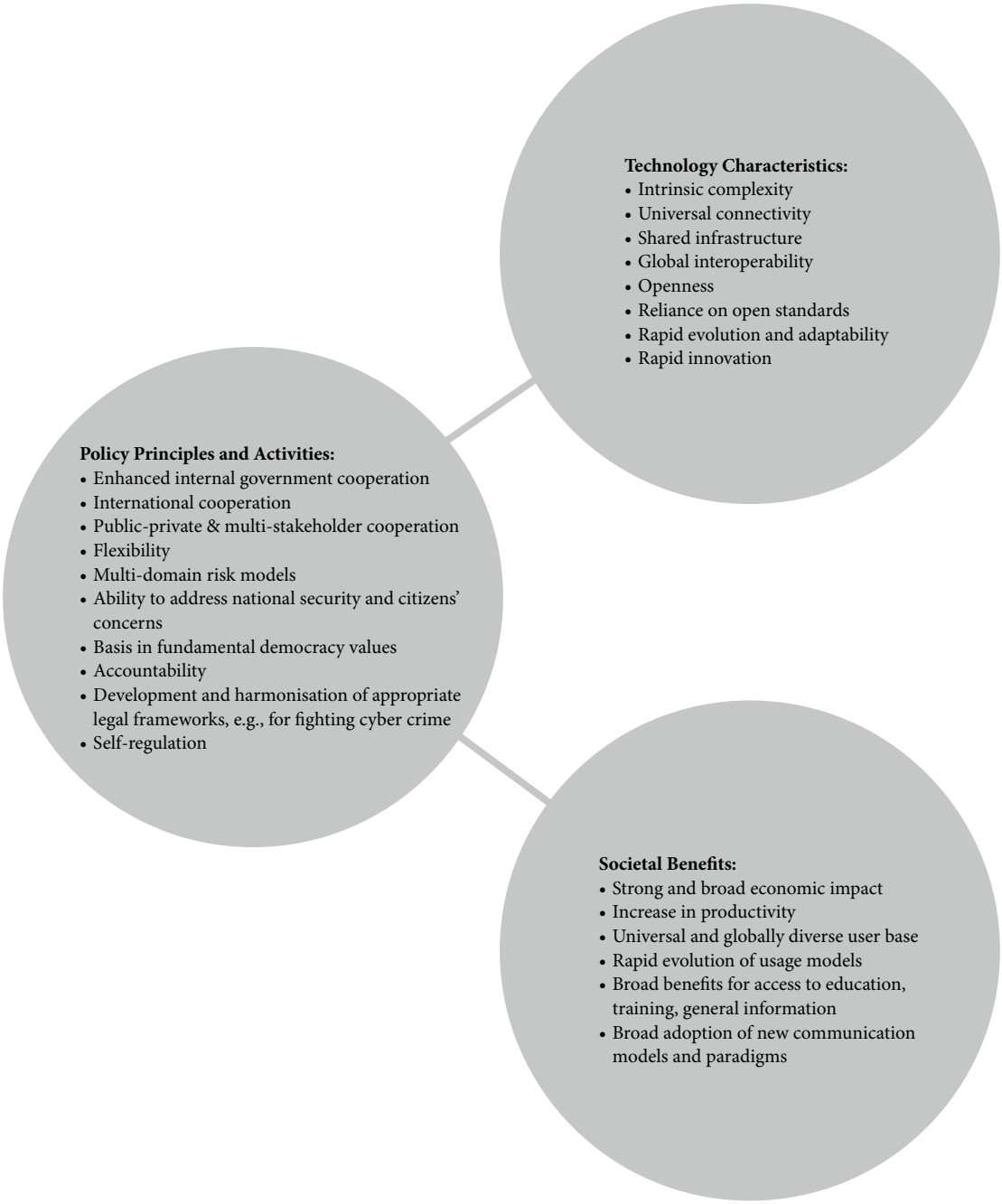


Figure 1. Consolidated graphic of key concepts and principles – high level of the proposed ontology.

approaches shared by cyber security strategies of multiple countries such as Information Sharing and Analysis Centre (ISAC) efforts.

Policies necessary to support the rapid development of the technology space and the societal benefits it fosters have to be based on the integrated characteristics of the cyber environments, and the attributes and principles upon which these characteristics are built. They need to include a well-defined connection between technology norms and best practices, and high-level policy principles. Such a connection is necessary in order to define policies and regulations in a way that makes them compatible with the technology environment. The meaning of key principles such as support for privacy or transparency needs to be reinforced by the link with technical and process best practices that is necessary to operationalise these concepts. A rich ontology linking principles with norms and best practices can help in maintaining a unified, but actionable model of cyberspace and in forming objective links between the layer of principles and the layer of norms and best practices.

6. Conclusions

The international harmonisation of cyber security strategies and visions has not yet been achieved, but the analysis of diverse literature on cyber security and cyberspace shows a degree of coherence for high-level concepts and displays evidence of commonality in concepts, principles, and attributes describing various aspects of policy, technology space, and societal impacts of cyberspace. This commonality provides a reservoir of fundamental concepts and principles that can help industry, government, academia, and others to develop an in-depth view of cyberspace.

These common concepts and principles covering technology, policy, and societal issues can serve as a foundation of a shared approach to cyber security devised as an ontology. The ontology could connect high-level principles developed by policy efforts and best practices designed by industry experts. It could be instrumental in creating a common context to support multi-stakeholder interactions, could help to model and predict the rapid pace of chance in cyberspace and could enable a multi-disciplinary scientific view of cyber security.

Although we did not build a prototype ontology to support the ontology proposal in this paper, such an ontology could be quickly developed based on the top-level concepts we proposed and with the use of common ontology tools such as Protégé[43] and based on the methodology described here. The development of such an ontology is a worthy topic for a multi-disciplinary community effort.

43 Protégé, http://protege.stanford.edu/.

Industry has developed a set of best practices and norms in cyber security, such as technology and governance standards, best practices for privacy and data protection, and secure technology development. They are based on high-level principles evolved by the global community. However, the connection between norms and principles remains abstract, hindering mutual understanding in multi-stakeholder initiatives and harmonisation efforts. We believe that an ontology permitting diverse stakeholders to reason about the complex environment can provide tools leading to greater mutual understanding and, as a result, to greater progress in cyber security initiatives.

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

APPENDIX 1

Cyber Security Norms Proposed by Microsoft[1]

1. Limiting and Managing Escalation of Threats in Cyberspace Through Norms

Cybersecurity norms that limit potential conflict in cyberspace are likely to bring predictability, stability, and security to the international environment – far more than any set of confidence-building measures (CBMs). With a wide acceptance of these norms, governments investing in offensive cyber capabilities would have a responsibility to act and work within the international system to guide their use, and this would ultimately lead to a reduction in the likelihood of conflict.

Conflict is often characterized as one of two discrete states: peacetime and war. In reality, whether talking about cyberspace or the physical world, there is an escalation path from more common (yet still complex) events that occur in peacetime, to increasing activity and incidents, disruptions, emerging conflict, conflict, and, eventually war, as shown in Figure 1. Different legal frameworks apply at these various stages.

International policy work to date has primarily focused on cybersecurity norms as a means to reduce risk from potentially complex cyber events at the national and regional levels and advance CBM efforts at the international level.

1 This Appendix is based on Angela McKay, et al, Microsoft Corporation, *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* (14 December 2014), http://www.microsoft.com/en-us/download/details.aspx?id=45031. Please note that these recommendations were published in December 2014, i.e. before the 2015 UN GGE report: 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.

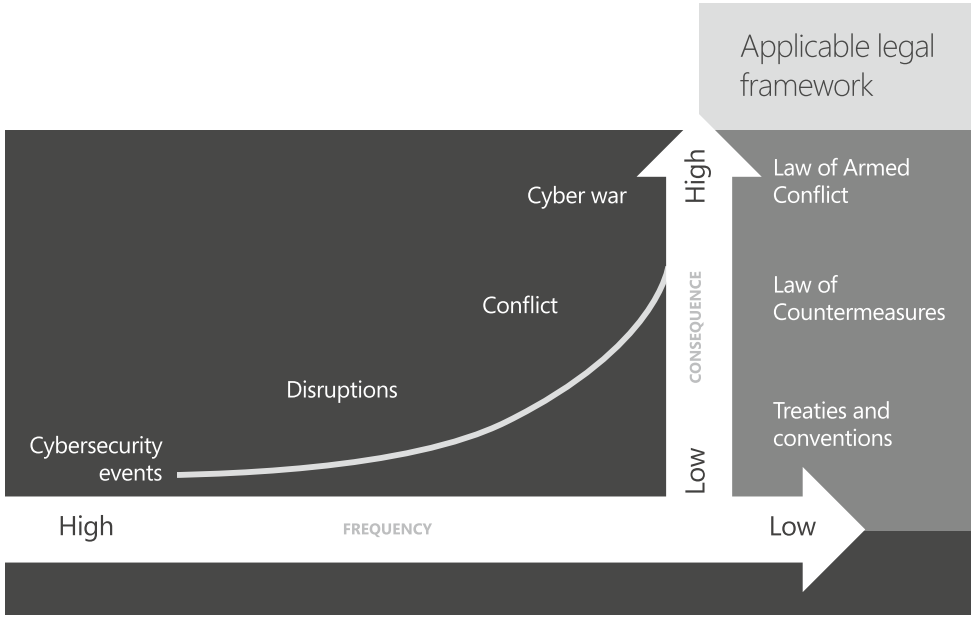


Figure 1. Escalation of cyber events and applicable legal frameworks.

Authorities have paid particular attention to risks and events where there is broad societal agreement on the most significant of issues that face the world – such as armed conflict, nuclear non-proliferation, global resources, and trade. With this alignment on acceptable and unacceptable objectives, actions, and impacts, it seems increasingly appropriate to address cybersecurity risks and events through treaties and conventions. Work to address cyber crime through increased international collaboration is one such example. Another example is the work within the UN, which has looked at a relatively narrow, but vital, segment of cyber conflict for events of extremely high consequence but low likelihood and which would be addressed under the Law of Armed Conflict.

To date, cyber events have not risen to the level of armed conflict. However, while the boundaries between crime and conflict in cyberspace are often hard to discern, events within that space can have broad societal impact, and be challenging to defend against. When existing diplomatic efforts are laid over the spectrum of possible events and applicable legal frameworks, the opportunity for greater development of cybersecurity norms to both improve defense, but in particular limit conflict, is apparent. Figure 2 below illustrates the area where the greatest opportunity for cybersecurity norms exist.

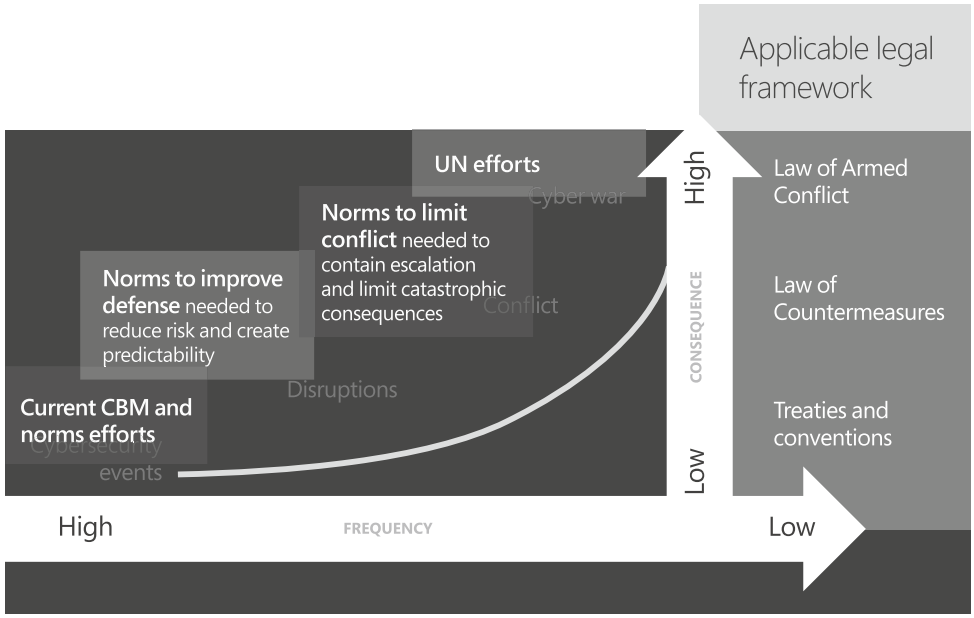


Figure 2. Opportunity space for cybersecurity norms.

2. Six Proposed Cybersecurity Norms to Limit Conflict

In light of the growing number of offensive capabilities, Microsoft believes that cybersecurity norms are needed to limit potential conflict in cyberspace and to better define what type of government behaviors in cyberspace should be 'out of bounds' so that events don't escalate to warfare. These norms should not only be designed to strengthen cybersecurity but also to preserve the utility of a globally connected society.

We believe that if cybersecurity norms are to be effective, they have to meet four key criteria. First, they must be practicable. They also need to reduce risks of complex cyber events and disruptions that could lead to conflict. In addition, they need to drive behavioral change that is observable and that makes a demonstrable difference in the security of cyberspace for states, enterprises, civil society, and individual stakeholders and users. Finally, effective norms should leverage existing risk-management concepts to help mitigate against escalation, and, if escalation is unavoidable, they should provide useful insight into the potential actions of involved parties.

To help catalyze progress on the development of effective cybersecurity norms, Microsoft proposes six norms to limit conflict. The proposed norms are intended to reduce the possibility that ICT products and services could be used, abused, or exploited by nation states as part of offensive operations that result in unacceptable impacts, such undermining trust in ICT; set boundaries for how cyber weapons

are developed, contained, and used; and create a meaningful global framework for managing vulnerabilities. We recognize that norms should not be an objective by themselves. Only if implemented, assessed for accountability, and, as appropriate, evolved, can they drive demonstrable changes in behavior.

NORM 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.

The global technology industry is founded on trust, in that consumers, enterprises, and governments depend on ICT for critical functions. Although the private sector can and does invest considerably in efforts to advance and demonstrate the assurance and integrity of products and services, states have the unique capability to direct disproportionately larger resources to exploit these products or services and to taint the broad ICT supply chains by which they are delivered. Exploiting of commercial off-the-shelf (COTS) products and services – which puts at risk every computer user dependent on that technology, even if that user is of no interest to a government – would be an action with the potential to create unacceptable impacts globally, since the degradation of trust in ICT would threaten innovation and economic security. Sophisticated state-resourced tradecraft targeting ICT companies to place backdoors or vulnerabilities in COTS products – or compromising signing keys to enable government to misrepresent the provenance of software – may exceed the commercially reasonable limits of the private sector operational security and integrity controls. Governments should also refrain from undermining international security standards efforts to benefit their own interests.

NORM 2: States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.

It is well-documented that governments around the world are active participants in the cyber vulnerability market and that they exploit gray and black markets.[2] The Heartbleed vulnerability, discovered in 2014, fueled additional speculation as to how governments stockpile vulnerabilities in ICT products rather than disclosing them to vendors to fix before they are exploited. In April 2014, in response to specific allegations against the US government, the White House published its framework approach to addressing if or when the federal government may withhold knowledge of a vulnerability from the public: 'This administration takes seriously its commitment to an open and interoperable, secure and reliable Internet, and in the

2 'The Digital Arms Trade: The Market for Software that Helps Hackers Penetrate Computer Systems,' *The Economist*, March 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. This has been and continues to be the case.'[3] The White House further noted that building up a 'huge stockpile of undisclosed vulnerabilities' while leaving the Internet vulnerable and people unprotected would not be in the national security interest of the United States.[4]

Although the White House reserved the right to use vulnerabilities as a method of intelligence collection, this approach does reflect a positive analysis that short-term gains to advance one objective could also create impacts that threaten other objectives, such as economic growth, technological innovation, and trust in government. We recommend that other governments similarly develop and publicly publish their policies on vulnerability handling and that they have a partiality for reporting vulnerabilities to vendors. When doing so, they should adhere to the principles of Coordinated Vulnerability Disclosure (CVD).

NORM 3: States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

Microsoft recognizes that governments will develop cyber weapons and protocols for their own use. When governments do build them, therefore, they should ensure that they are building cyber weapons that are controllable, precise, and not reusable by others, consistent with the concepts of distinction, discrimination, and distribution previously discussed, to limit the impacts associated with these actions.

NORM 4: States should commit to nonproliferation activities related to cyber weapons.

As states increase investments in offensive cyber capabilities, care must be taken to not proliferate weapons or techniques for weaponizing code. States should establish processes to identify the intelligence, law enforcement, and financial sanctions tools that can and should be used against governments and individuals who use or intend to use cyber weapons in violation of law or international norms. Furthermore, states should agree to control the proliferation of cyber weapons in cooperation with international partners and, to the extent practicable, private industry. Implementing this norm will not only help limit state actions that could have unacceptable impacts but also will help reduce the possibility that cyber weapons could be used by non-state actors.

NORM 5: States should limit their engagement in cyber offensive operations to avoid creating a mass event.

3 Michael Daniel, 'Heartbleed: Understanding When We Disclose Cyber Vulnerabilities,' *White House Blog*, April 28, 2014, http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

4 Ibid.

Governments should review and update their current policy positions with an appreciation for the unintended consequences or impacts in cyberspace that could escalate conflict, incite war or disproportionately harm civilian ICT. During an armed conflict, as regulated by the law of war, any attack must be justified by military necessity, intended to help in the military defeat of the enemy, with a military objective. Furthermore, the harm caused to civilians or civilian property must be proportional in relation to the concrete and direct military advantage anticipated. In other words, the action should be to advance defined and accepted military objectives and should not create disproportional impacts. These strictures can and should be applied to offensive cyber operations. States should recognize that attacks targeting the confidentiality, integrity, or availability of ICT systems, services, and data can have a mass effect beyond any reasonable sense of proportionality and required global action.

NORM 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Although governments play an increasingly important role in cyberspace, the first line of defense against cyber attacks remains the private sector, with its globally distributed telemetry, situational awareness, and well-established incident response functions. There has not been evidence of governmental interference with private sector recovery efforts following a severe cyber attack, but governments should commit to not interfere with the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs), individual response personnel, and technical response systems. Intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals.

Additionally, governments should go one step further and, when asked by the private sector, commit to assist with recovery and response needs that have global and regional implications. For example, repairing cuts in underwater sea cables often requires permits and cross-border movement of technical equipment or experts, and governments can help ensure that those actions are expedited. Alternatively, a cyber event with large-scale impacts, such as the Shamoon attacks in 2012,[5] could require the rapid movement of hardware from one place to another, the need for international technical collaboration between and among governments and the private sector, and the waiving of legal barriers in times of national emergency to facilitate recovery.

5 Jack Clark, 'Shamoon Malware Infects Computers, Steals Data, Then Wipes Them,' *ZDNet*, August 17, 2012, http://www.zdnet.com/shamoon-malware-infects-computers-steals-data-then-wipes-them-7000002807/.

Biographies

Shireen Alam is a Research Assistant with Symantec's Global Government Affairs team based in Washington DC. Before joining Symantec, Shireen worked for the Committee on Homeland Security (minority staff) at the United States House of Representatives and holds a law degree.

Greg Austin is a Professor of Cyber Security, Strategy and Diplomacy at the University of New South Wales Canberra and a Professorial Fellow with the EastWest Institute in New York. He has published seven books on international security, including 'Cyber Policy in China' (Polity 2014) which he wrote while a Senior Visiting Fellow at the Department of War Studies in Kings College London. His publications include articles on cyber peace, cyber relations among the great powers, and the cyber policy of middle powers. He is co-author with Sandro Gaycken of a report, 'Resetting the System: Why Highly Secure Computing Should be the Priority of Cyber Security Policies' (EastWest Institute 2014). As co-chair of EastWest's Breakthrough Group on Measures of Restraint in Cyber Space, he co-authored their recent report, 'Promoting International Cyber Norms: A New Advocacy Forum' (2015). He set up an innovative Master's degree on cyber war and peace at UNSW.

Russell Buchan is a Senior Lecturer in International Law at the University of Sheffield. Russell sits on the editorial board of the Journal of the Use of Force in International Law and the International Community Law Review. Russell's monograph was published by Hart Publishing in 2013 and is entitled 'International Law and the Construction of the Liberal Peace', and was the recipient of the American Society of International Law's Francis Lieber Prize for an outstanding monograph in the field of the

law of armed conflict for 2014. Russell has co-edited, along with Professor Nicholas Tsagourias, an edited collection entitled 'A Research Handbook on International Law and Cyberspace', published by Edward Elgar. Russell has also recently signed a book contract with Hart Publishing entitled Cyber Espionage and International Law. Russell is Co-Rapporteur for the International Law Association's Study Group on Cybersecurity, Terrorism and International Law.

Madeline Carr is a Senior Lecturer in International Relations at Cardiff University. She has been funded by the British Academy to undertake research on the role of the public/private partnership in national cyber security strategies. She is part of the UK's £10M research hub on the cyber security of the Internet of Things. Madeline's research is embedded in a broad study of the ways in which new technology both reinforces and disrupts conventional frameworks for understanding International Relations and the implications of this for state and global security, order and governance. She was selected in 2014 for the Welsh Crucible as a future research leader and is a multi-award winning teacher. Madeline is on the executive committee for the newly established ISA section STAIR (Science, Technology and Arts in International Relations) and is the 2016 co-program chair. Madeline has published on Internet Freedom and multi-stakeholder Internet governance and her book 'US Power and the Internet in International Relations' is published with Palgrave MacMillan.

Ilias Chantzos is Senior Director of Symantec's Government Affairs programmes for Europe, Middle East & Africa (EMEA) and Global Advisor for Critical Infrastructure and Data Protection. Chantzos represents Symantec before government bodies, national authorities and international organisations advising on public policy issues with particular regard to IT security and privacy. Before joining Symantec in 2004, Chantzos worked as legal and policy officer in the Directorate General Information Society of the European Commission focusing on information security policy. He covered the Council of Europe Cybercrime Convention and the Framework Decision on Attacks against Information Systems. In addition, he worked on a number of EU legislative initiatives relevant to information society and security. He also represented the European Commission in

various international debates and conferences. Chantzos holds a law degree, a Masters degree in Computers and Communication Law and a Master degree in Business Administration.

Toni Erskine is currently Professor of International Politics at the University of New South Wales, Australia, and Associate Director (Politics & Ethics) of its Australian Centre for Cyber Security. She has recently served on the Governing Council (2014–16) and Executive Committee (2014–15) of the International Studies Association, and is past President of its International Ethics Section (2008-10). Until 2013 she was Professor of International Politics at Aberystwyth University, UK, where she was awarded a Personal Chair in 2009. She has been British Academy Postdoctoral Fellow at Cambridge University, Lurie-Murdoch Senior Research Fellow in Global Ethics and Honorary Professor at RMIT University in Melbourne, and Visiting Scholar at Sydney University. Her books include: 'Embedded Cosmopolitanism: Duties to Strangers and Enemies in a World of Dislocated Communities' (Oxford University Press, 2008); with Richard Ned Lebow, 'Tragedy and International Relations' (Palgrave Macmillan, 2012); and, with Ken Booth, 'International Relations Theory Today' (Polity, 2016). She is currently completing a book entitled 'Locating Responsibility: Institutional Moral Agency and International Relations'.

Marina Kaljurand has served as the Minister of Foreign Affairs of the Republic of Estonia since 16 July 2015. She is not affiliated with any political party. Marina Kaljurand has been in the diplomatic service since 1991, when she started her career as the III secretary of the Press and Information Department. She has worked as Director of the International Treaties Division (1991-1996) and as a counsellor at the Estonian Embassy in Helsinki (1996-1999). From 2002 to 2005, she worked as the Undersecretary for Legal and Consular Affairs. She has served as Ambassador to the following states: the State of Israel (non-resident, 2004-2006), the Russian Federation (2005-2008), the Republic of Kazakhstan (non-resident, 2007-2011), Canada (non-resident, 2011–2013), the United Mexican States (non-resident, 2011–2014) and the United States of America (2011-2014). From October 2014 to May 2015, she held the position of Undersecretary for Political Affairs. From 1992 to 1994, Marina Kaljurand was the legal expert of the Governmental Delegation regarding

the Agreement on Troops Withdrawal between Estonia and the Russian Federation. From 2002 to 2004, she was a member of the Governmental Delegation regarding accession negotiations to the European Union and head of the Legal Working Group of the Accession Treaty. She was also a Chief Negotiator on the accession of Estonia to the OECD in 2008-2011 and an Estonian Cyber Security Expert at the UN Group of Governmental Experts on Cyber Security from 2014 to 2015. Marina Kaljurand has a M.A. in law from the University of Tartu. She has also graduated from the Estonian School of Diplomacy and has an M.A. in international law and diplomacy from Tufts University's Fletcher School of Law and Diplomacy.

Mihoko Matsubara is Cyber Security Policy Director, Intel K.K., Tokyo. She previously served the Japanese Ministry of Defense for nine years, working with the US government, until she left to pursue her MA in International Relations and Economics on Fulbright at the Johns Hopkins School of Advanced International Studies in Washington DC. Upon graduation, she worked at Pacific Forum CSIS as a Fellow to research Japan-US cyber security cooperation. After she returned to Tokyo, she worked at Hitachi Systems as a Cyber Security Analyst on geopolitical risks and policy issues. She has been actively publishing articles, blogs, and papers including ones from the Council on Foreign Relations and the RUSI Journal. She provided a talk about international cyber security cooperation on a panel at the NATO CCD COE International Conference on Cyber Conflict 2015.

Paul Meyer is an Adjunct Professor of International Studies and a Fellow in International Security at Simon Fraser University and a Senior Fellow at The Simons Foundation, both in Vancouver, Canada. A former career diplomat, Paul served as Canada's Ambassador and Permanent Representative to the UN and Conference on Disarmament in Geneva (2003-2007) as well as the Director-General of the Security&Intelligence Bureau of the Department of Foreign Affairs (2007-2010). An exponent of conflict prevention through diplomacy he has written extensively on issues of international cyber security and outer space security.

Anna-Maria Osula is a Senior Analyst in the Law and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence. During her time with the Centre she has worked with projects like CyCon,

Cyber Coalition, Locked Shields, and published research on national cyber security strategies, international organisations, international cooperation and cyber defence. During 2013-2015, she was the lead for the 'Cyber Norms' project. She is also a Lecturer at the Tallinn Technical University Cyber Defence Master Programme, and a frequent presenter at international conferences. Anna-Maria holds an LLM degree in IT Law from Stockholm University and is working towards a law PhD at Tartu University, Estonia.

Patryk Pawlak is a Policy Analyst at the External Policies Unit of the Members' Research Service where he deals primarily with questions related to cybersecurity and terrorism. Before joining the European Parliament, Patryk was a Senior Analyst at the European Union Institute for Security Studies (EUISS) in Paris where he managed several projects, including the EUISS Cyber Task Force and EU-US Task Force on Transatlantic Strategies in the Asia-Pacific Region. During his career, Patryk has cooperated with numerous research institutions, universities and international organisations. His work on cyber-related issues, terrorism and European Union's security policies has appeared in several peer-reviewed journals and edited volumes. In 2014, he edited a report 'Riding the digital wave – The impact of cyber capacity building on human development' published by EUISS. Patryk holds a PhD in Political Science from the European University Institute in Florence.

Audrey L. Plonk is the Director of Global Cybersecurity and Internet Governance Policy at Intel Corporation. Audrey leads a global team of policy experts focused on Internet policy issues and governance, cybersecurity and privacy. Prior to joining Intel in 2008, Audrey worked for the Organization for Economic Co-operation and Development (OECD) based in Paris, France. Audrey led the OECD's security policy work on critical information infrastructure protection and malware. From 2003 to 2006, Audrey worked as a consultant for the US Department of Homeland Security's National Cyber Security Division, primarily focusing on international security policy issues in their International Affairs Division. Audrey attended The George Washington University in Washington, DC and received her B.A. in International Affairs with a focus on the European Union and received a double minor in French and dance.

Henry Rõigas is an Analyst in the Law and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence. His research in the Centre focuses mainly on the political aspects of international cyber security. Henry is responsible for the Centre's INCYDER (International Cyber Developments Review) database, co-organises CyCon and was the Project Manager of the book 'Cyber War in Perspective: Russian Aggression against Ukraine'. Henry holds a Master's degree in International Relations from the University of Tartu.

Michael Schmitt is Charles H. Stockton Professor and Director of the Stockton Center for the Study of International Law at the United States Naval War College. He is also Professor of Public International Law at Exeter University; Senior Fellow of the NATO Cooperative Cyber Defense Centre of Excellence; Fellow at Harvard Law School's Program on International Law and Armed Conflict; and Director of Legal Affairs with Cyber Law International.

Claire Vishik's work at Intel Corporation focuses on hardware security, trusted computing, privacy enhancing technologies, encryption and related policy issues. Claire is a member of the Permanent Stakeholders Group of ENISA, the European Network and Information Security Agency. She is active in standards development and is on the Board of Directors of the Trusted Computing Group, Council of the Information Security Forum, and a co-chair of NIST Public Working Group on Cyber-Physical Systems. She is engaged in work on R&D strategies in Europe and the US and is an advisor to a number of R&D projects and initiatives. Claire received her PhD from the University of Texas at Austin. Prior to joining Intel, Claire worked at Schlumberger Laboratory for Computer Science and AT&T Laboratories. Claire is the author of numerous peer reviewed papers and reports and inventor of 30+ pending and granted US patents.

Liis Vihul is a Senior Analyst in the Law and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence and the CEO of Cyber Law International. She holds Master's degrees in law from the University of Tartu and in information security from the University of London. Her research focuses on the interplay between public international law and cyber operations. Ms.

Vihul co-authored the book 'International Cyber Incidents: Legal Considerations'. She was also the Manager of the project that resulted in the 'Tallinn Manual on the International Law Applicable to Cyber Warfare' and serves in the same role for its follow-on project, 'Tallinn 2.0'.

Sean Watts is a Professor of Law at Creighton University Law School. He is also a Senior Fellow with the NATO Cooperative Cyber Defence Center of Excellence in Tallinn, Estonia and serves as a US Army Reservist at the U.S Strategic Command. His scholarship focuses on international legal regulation of emerging forms of warfare. He served as a Group Facilitator for the Tallinn Manual on International Law Applicable to Cyber Warfare and is involved in a revised and expanded edition of the Manual. From 2009-12, he served as a defense team member in *Gotovina et al.* at the International Criminal Tribunal for Former Yugoslavia. He is co-founder of the Nuremberg to Hague (N2H) International Criminal Law Summer School Program conducted each year in Germany, the Netherlands, and Poland. Prior to teaching, Professor Watts served both as an active-duty Army Judge Advocate and an Armor officer in a tank battalion.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu