Civil Society and Disarmament
2017

Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology

A Commentary

UNODA
United Nations Office for Disarmament Affairs

UNODA

United Nations Office for
Disarmament Affairs

CIVIL SOCIETY AND DISARMAMENT
2017

Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology

A Commentary

United Nations

Note

The United Nations Office for Disarmament Affairs is publishing this material within the context of the United Nations Disarmament Information Programme in order to further an informed debate on topical issues of arms limitation, disarmament and security. This publication series aims to give civil society a platform for their views on disarmament-related matters.

The material appearing in this book is in unedited and original form as submitted by the authors. The views of the authors are their own and do not necessarily reflect those of the United Nations or its Member States.

Symbols of United Nations documents are composed of capital letters combined with figures. These documents are available in the official languages of the United Nations at http://ods.un.org. Specific disarmament-related documents can also be accessed through the disarmament reference collection at https://www.un.org/disarmament/publications/library/.

This publication is available at

www.un.org/disarmament

UNITED NATIONS PUBLICATION
Sales No. E.18.IX.3

ISBN 978-92-1-142326-6
eISBN 978-92-1-363102-7

Contents

Recommendations contained in paragraph 13 of the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should 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;

(b) 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;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) 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. States may need to consider whether new measures need to be developed in this respect;

(e) 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 General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State 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;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) 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;

(i) 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;

(j) 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;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Foreword

It has been a great pleasure to work with Dr. Eneken Tikk to launch this call for comments by scholars and practitioners on the list of recommendations of responsible state behavior in cyberspace suggested in the reports of the United Nations Group of Governmental Experts (GGE) and how to operationalize them in practice.

Given the accelerating deterioration of international relations, including global cyber relations, it has become most urgent that international norms of responsible state behavior be adopted and adhered to by all states and non-state actors. The United Nations GGE reports have developed and suggested a very useful set of norms, that should be adopted urgently and universally, to prevent a major escalation of malicious and self-destructive cyber activities by governments and non-state actors.

ICT4Peace has been concerned with Peace and Security in the Cyberspace since its inception in 2004 in the context of the United Nations World Summit on the Information Society in Geneva and Tunis. While championing the use of information and communications technologies (ICTs) for peaceful purposes including peace building and humanitarian operations, ICT4Peace at the same time endeavored to contribute to the maintenance of a peaceful, secure, open and trusted cyberspace, through policy research, advocacy and capacity building activities. I have been privileged to work with and be supported by such eminent scholars such as Mr. Sanjana Hattotuwa, Dr. Eneken Tikk, Dr. Camino Kavanagh, Dr. Mika Kerttunen, former Ambassador Paul Meyer and Barbara Weekes to mention just a few.

In response to rapidly emerging threats and risks for the cyberspace, not only by crime, hackerism and terrorism but also for strategic purposes, in June 2011 ICT4Peace called publicly for a code of conduct or norms for responsible state behavior, as well as Confidence Building Measures (CBMs) for a peaceful and secure Cyberspace. I think it is safe to say, that the world community was pleased to see that key states were finally able to agree on a set of recommendations for norms and CBMs at the 2013 and 2015 reports of the United Nations GGE on cybersecurity, but also at regional fora such as the OSCE and the Asian Regional Forum. These very useful diplomatic results have to be espoused and operationalized universally by all States, big or small, be they developing or developed countries.

This publication's main objective is to support this process.

Daniel Stauffacher
Founder and President of the ICT4Peace Foundation
Former Ambassador of Switzerland

Preface

This commentary is a synthesis of views and perspectives. In an open call for comments, the editors invited scholars, experts and enthusiasts to submit recommendations, comments and guidance for understanding and interpreting the recommendations of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Most of the contributors and lead editors have never been exposed to the GGE process and have therefore taken the Group's recommendations at face value.

More than 40 scholars and experts were involved in drafting this commentary, and these authors contributed their views on all or part of the recommendations in line with their respective areas of expertise, interest and experience. The lead editors then compiled and synthesized the contributions and added a broader contextualization and analysis of each recommendation.

Each chapter follows the same structure, beginning with a section that places one of the recommendations in the broader context of the 2010, 2013 and 2015 GGE reports and applicable national submissions. In the background section that follows, commentators highlight various elements of the evolution and discussion of the issue(s) addressed in the recommendation in question. An expansion segment offers additional perspectives and approaches, feeding into further analysis. The chapter then concludes with proposals that, in the lead editors' view, are essential for implementing the recommendation under consideration.

This publication does not claim to be exhaustive or even correct. Rather, it is a compilation of views intended to

inform the implementation of the Experts' brief and laconic guidance. Thus, the commentary presents possible means for the recommendations to be understood, emphasized and discussed. Accordingly, it should be regarded not as an authoritative document, but as an invitation to exchange views and perspectives in pursuit of a more uniform and common understanding of the issues and solutions that the 2014/2015 GGE addressed in its eleven recommendations.

This volume of the Civil Society and Disarmament series was prepared in cooperation with ICT4Peace, a policy and action-oriented international foundation that aims to save lives and protect human dignity through information and communication technology (ICT). Since 2004, ICT4Peace has explored and has championed the use of information and communications technologies (ICTs) and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007, ICT4Peace has promoted cybersecurity and a peaceful cyberspace through, inter alia, international negotiations with governments, international organizations, companies and non-state actors.

Eneken Tikk
Editor-in-Chief

Acknowledgements

We would like to thank the following contributors to this publication:

Prof. Robert Barnsby, Department of Law, United States Military Academy at West Point

Dr. Serge Droz, Vice President Computer Emergency Response Team at Open Systems

Yves Duguay, President of HCiWorld and former Senior VP, Screening Operations at the Canadian Air Transport Security Authority, Canada

Prof. Myriam Dunn-Cavelty, Center for Security Studies, ETH Zürich

Prof. Vittorio Fanchiotti, University of Genoa

Dr. Guido Gluschke, Co-Director and Senior Research Fellow, Institute for Security and Safety, Brandenburg University of Applied Sciences, Germany

Miguel Alberto N. Gomez, Center for Security Studies, ETH Zürich

Dr. Richard Hill, independent consultant

Tyson Johnson, Chief Operating Officer, Cyber New Brunswick, Canada

Dr. Mika Kerttunen, Cyber Policy Institute

Amb. Kriangsak Kittichaisaree, Judge of the International Tribunal for the Law of the Sea

Dr. Tang Lan, Institute of Information and Social Development, China Institutes of Contemporary International Relations

Prof. Peter Margulies, Roger Williams University School of Law

Dr. Tim Maurer, Cyber Policy Initiative, Carnegie Endowment for International Peace

The Microsoft Corporation

Dr. Anja Mihr, Center on Governance through Human Rights, HUMBOLDT-VIADRINA Governance Platform

Robert Morgus, New America's Cybersecurity Initiative

Vivian Ng, Senior Research Officer, Human Rights, Big Data and Technology Project, University of Essex

Prof. Nohyoung Park, Cyber Law Centre at Korea University

Lorenzo Picotti, Department of Law, University of Verona

Dr. Jean Paul Pierini, Officer, Italian Navy

Prof. Yuval Shany, Hersch Lauterpacht Chair in Public International Law, Faculty of Law, The Hebrew University of Jerusalem

Francesca Spidalieri, Senior Fellow for Cyber Leadership, Pell Centre, Salve Regina University, United States of America

Dr. Anatoly A. Streltsov, Information Security Institute, Moscow State University

Dr. Eliza Watt, Lecturer in Law, Bournemouth University

Prof. Thomas C. Wingfield, College of Information and Cyberspace of the National Defense University (United States of America)

This project would not have succeeded without the energy and assistance of Walle Bos. We are also indebted to the Institute of Security and Global Affairs of Leiden University for providing the first home for this project.

Finally, we would like to thank the Kingdom of the Netherlands and the Federal Republic of Germany for their important support to make this publication possible.

- *Authors*

Introduction

Eneken Tikk

The issue of cybersecurity is no stranger to any state or organization these days. With the increasing dependence of societal, economic and political affairs on information and communication technologies (ICTs), safety and security in the use of these technologies has become an acute issue.

International cybersecurity is a subset of cybersecurity issues that focuses on international peace and security considerations the development and use of ICTs may have or create. Since 1998, under the Russian initiative, the United Nations First Committee has been discussing the actual and potential threats that state use of ICTs may bring to international peace, security and stability under the resolution on developments in the field of information and telecommunications in the context of international security.[1] In this discussion, many states have shared their views on respective issues and applicable measures.[2] As part of the

---

[1] *Developments in the field of information and telecommunications in the context of international security*, Resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, 70/237 of 23 December 2015 and 71/28 of 9 December 2016.

[2] *Developments in the Field of Information and Telecommunications in the Context of International Security,* Reports of Secretary-General containing replies received from Governments (A/54/213; A/55/140 and Corr.1 and Add.1; A/56/164 and Add.1; A/57/166 and Add.1; A/58/373; A/59/116 and Add.1; A/60/95 and Add.1; A/61/161 and Add.1; A/62/98

First Committee process, five Groups of Governmental Experts (GGE) have convened since 2004 to study the matter under the mandate formulated by the General Assembly. On consensus basis, Experts offer their recommendations as to what constitutes responsible state behaviour in the use of ICTs in the context of international peace and security.[3]

The fourth Group, working through four week-long sessions in 2014/2015, recommended that states could consider voluntary, non-binding norms for responsible state behavior to increase stability and security in the global ICT environment.[4] The Group concluded that such norms could reduce risks to international peace, security and stability. Such norms, the Group emphasized, would not seek to limit or prohibit action that is otherwise consistent with international law. Instead, norms reflect the expectations of the international community, set standards for responsible state behavior and allow the international community to assess the activities and intentions of States. This way, 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.

The Group saw as their task to determine where already existing norms may be formulated for application to the ICT environment, encourage greater acceptance of existing norms and identify where additional norms may need to be developed taking into account the complexity and unique attributes of ICTs.

In this context, the achievement of the Group is remarkable. Coming from very different countries, some of

---

and Add.1; A/64/129 and Add.1; A/65/154; A/66/152 and Add.1; A/67/167; A/68/156 and Add.1; A/69/112 and Add.1; A/70/172 and Add.1).

[3] For a detailed discussion of the First Committee process and the work of the GGEs, see Tikk and Kerttunen (2018) The Alleged Demise of the United Nations GGE: An Autopsy and Eulogy (www.cpi.ee).

[4] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174).

whom having diametrically differing views on the preferred role and functions of ICTs in global and national life, Experts joined efforts in issuing recommendations that they believed to improve the situation of international cybersecurity. In doing so, they put aside their differences and focused on their shared goal: an open, free, secure and stable cyberspace.

The work of the United Nations GGE has received considerable support and attention. The General Assembly has called United Nations member states to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts. G20 has also invited states to implement the GGE recommendations: "all states should abide by norms of responsible state behavior in the use of ICTs."[5] In 2017, G7 listed all eleven recommendations in their Lucca declaration.[6]

As the GGE works in closed sessions, much in the Group's report is left subject to interpretation. To invite wider, potentially universal, adherence to the GGE recommendations, this commentary invites a broader and deeper discussion on the recommendations. This commentary offers some views to how the Experts' guidance may be understood and implemented. This reservation entails that there are, and should be, additional views and considerations and that it is important that the international community keeps studying, debating and revising the guidance with the view to finding their respective preferences as to how to benefit from the recommendations.

One very particular debate about the 2015 recommendations deserves a separate comment. Ever since the GGE came to discuss norms pertaining to state use of ICTs, there has been a slight confusion about what exactly is meant by *norms* in this discourse. Initially, norms became seen as a type of measure to address existing and potential threats in the sphere of information security.[7] The 2009/2010 Group recommended

---

[5] *G20 Leaders' Communiqué*, 15-16 November 2015.

[6] *G7 Declaration on responsible state behavior in cyberspace*, 11 April 2017.

[7] Resolution 60/45 of 6 January 2006 (A/RES/60/45).

"further dialogue among States to discuss norms pertaining to State use of ICTs".[8] In the 2010 setting, there was no clarity as to whether such norms would derive from existing international law or constitute a new set of standards of behavior.

The 2012/2013 Group's mandate broadened the discussion of normative measures to norms, rules or principles of responsible behavior.[9] The 2013 GGE report concluded "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".[10] The Group also stated "common understandings on how such norms shall apply to State behavior and the use of ICTs by States required further study". It further maintained, "given the unique attributes of ICTs, additional norms could be developed over time".[11]

The 2014/2015 GGE was called "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 or principles of responsible behavior of States".[12] An additional element in the mandate was a request to study "how international law applies to the use of information and communications technologies by States".[13]

Such slicing and bucketing of the norms discussion in the GGE has been subject to some confusion among observers. In particular, questions have been asked about the relationship between new norms, rules and principles and the already existing legal and policy instruments. Readers of this

---

[8] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 30 July 2010 (A/65/201).

[9] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98).

[10] Ibid., para. 16.

[11] Ibid.

[12] A/70/174.

[13] Ibid.

commentary may have already encountered a discussion[14] of the normative status of the GGE guidance, featuring diverging views:

(a) A view, whereby the recommendations of the 2015 GGE, although often referred to as "norms", do not have actual normative status as they have to be yet accepted as norms. This reading is correct if the GGE framing of their recommendations is taken at face value. Proponents of this view highlight the "weak" status of the recommendations and express discontent with their anticipated impact. However, as one leading GGE expert has explained, the GGE recommendations, even once accepted as norms, are not intended to deter the behavior of determined malicious and hostile actors. Instead, the Group seems to value the "soft" instrument of norms as a way to increase common understanding of the steps necessary to increase coherence in well-meaning states' behavior and cultivate a joint culture of international cybersecurity.

(b) A contradicting view, whereby at least some of the recommendations are presented as voluntary and non-binding, derive from or reflect international law and are therefore misplaced in the "norms" section. This understanding is prevalent among international law scholars. In the commentary, the reader will see strong emphasis on the already established legal status and practice of inter-state cooperation, state responsibility and due diligence. However, this reading also highlights the significant differences among countries about the binding status of certain instruments and rules of international law.

(c) Still another view, whereby there is no clear ordering principle in para. 17 of the 2015 report that would allow

[14] See, for instance, Dan Ward and Robert Morgus, Professor Cy Burr's Graphic Guide to: International Cyber Norms, 2014. See also Melissa Hathaway, Getting beyond Norms When Violating the Agreement Becomes Customary Practice, CIGI, 2017; Michael N. Schmitt and Liis Vihul, The Nature of International Law Cyber Norms, CCD COE Tallinn Paper No. 5, 2014.

a reader to identify the recommendations of the Group as aspirational, or as deriving from existing international law. Such reading is adopted as basis of this commentary, emphasizing that absent any particular guidance as to the normative status of the recommendations, states are free to decide how to best implement them. For instance, the US Cyber Diplomacy Act identifies several of the recommendations of the GGE as accepted norms.[15]

It is the view of the editor-in-chief of this commentary that while all the views can be substantiated and have merit for further discussion as to how to increase normative clarity and predictability around responsible development and use of ICTs, these considerations should not overcast the content of the GGE recommendations. The purpose of this commentary is not to resolve the unfortunate lack of clarity around the normative status of the GGE recommendations. For the purpose of this commentary, recommendations made by twenty experts in the 2015 report are taken at their face value—as recommendations, aimed at being accepted by the international community as standards of responsible state behavior in uses of ICTs and implemented at the national, regional and international levels.[16]

As the reader will observe, there will be different ways in which the recommendations could be understood, interpreted and implemented. Depending on a particular country's reading of international law, some of the experts' recommendations are reflective of already established legal standards that are, for reasons or others, not (yet) shared by all states. Other recommendations would require additional normative efforts at the national level, whereas some would require acknowledgment and collective implementation globally.

---

[15] https://www.gpo.gov/fdsys/pkg/BILLS-115hr3776rfs/pdf/BILLS-115hr3776rfs.pdf, Sec. 3 (b) 5 (A)-(I).

[16] For example, Germany advocates developing broad, non-contentious, politically binding norms of State behavior in cyberspace. They should be acceptable to a large part of the international community and should include measures to build trust and increase security. A/68/156/Add. 1, page 7.

To focus on the main purpose of the 2015 recommendations—to become accepted as norms—this commentary adopts a reading where conceptual clarity should not be made hostage to understanding the need for additional efforts to mainstream measures to reduce risks to international peace, security and stability.[17]

All recommendations in the 2015 report can be read as serving the purpose of filling in the gaps in existing instruments and practices. It is less relevant whether such gaps are mitigated in international or national law, or whether their implementation occurs by binding or non-binding instruments. What is essential is that states pay attention to the issues shared and raised by experts with relatively diverse views and preferences as to the development of information society and maintaining an open, free, secure and peaceful cyberspace.

In this reading, the 2015 GGE provides the international community with a very valuable roadmap to strengthening international cybersecurity. Debates about and between appropriate disciplines for capturing, adapting or introducing *norms* should belong to the implementation phase, rather than be built as a cipher for reading the recommendations in the first place.

To maximise shared understanding and joint efforts in achieving international cybersecurity goals, the GGE recommendations could be further compared with measures recommended by the Organization for Security and Co-operation in Europe (OSCE). OSCE, too, has considered it worthwhile to offer a set of voluntary, non-binding measures that, when implemented at the national level, would enhance interstate co-operation, transparency, predictability, and stability

[17] A/68/98, page 8. See also Michele Markoff, the US lead expert in the GGE, comments: What we need to do is consolidate what we've done and get states to implement," she said, "both in the internalization of the norms but also in the operationalization of [confidence-building measures] which will help the norms. http://www.defenseone.com/technology/2017/02/us-does-about-face-new-cyber-norms/135227/?oref=d-channelriver

and reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

There is hardly any state, even among those having participated in the OSCE and GGE discussions, that to date fully implements all the GGE recommendations. The time is ripe, therefore, to intensify international dialogue on responsible state behavior in the context of ICTs, and to exchange views about how to best implement the recommendations as well as to discuss further measures that, when universally accepted, would contribute to an open, secure, stable, accessible and peaceful ICT environment.

Recommendation 13 (a)

> *Consistent with the purposes of the United Nations, including to maintain international peace and security, States should 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.*

Zine Homburger

Contextualization

1. Recommendation (a) directly relates to the United Nations Charter. According to Art. 1 (1) and (3) of the United Nations Charter, the purposes of the United Nations are, inter alia, "to take effective collective measures for the prevention and removal of threats to the peace" and "to achieve international cooperation in solving international problems". To this end, the tasks of the General Assembly are to "initiate studies and make recommendations for the purpose of promoting international cooperation in the political field".[1] This mandate emphasizes the importance of cooperation within the United Nations. As Streltsov notes, the discussed recommendation "essentially expresses the underlying mechanism of the United Nations functioning, all activities of which in any field are based on cooperation of the member states of the Organization."[2]

---

[1] United Nations, *Charter of the United Nations*, 24 October 1945, (1 UNTS XVI), Art. 13 (1).

[2] Contribution by Anatoly A. Streltsov, page 10, para. 2.

Cooperation can be seen the prerequisite for any norm and agreement between states in any field of international relations.

2. Cooperation between states is the most fundamental requirement to meet the threats outlined in the United Nations GGE report of 2015. It is the basic assumption that such transboundary threats cannot be prevented and mitigated by states acting individually. Consequently, recommendation (a) should not be read as a stand-alone norm but rather forms the base for implementing the more specific recommendations of the 2015 report.[3] This is because any form of transboundary activities presupposes coordinated action between states as to achieve a specific objective. Therefore, recommendation (a) reflects a shared understanding with regard to the broader framework of cooperative measures.

3. The recommendation, furthermore, relates to several other parts of the 2015 report. Cooperation can be defined as a process of working together in order to achieve a certain end.[4] In more general terms, cooperation can be referred to as collective action in pursuit of a common goal.[5] For instance, confidence-building measures entailing elements of assistance and information sharing directly rely on cooperation as they encourage states to establish points of contact, initiate consultations and share their national views and information.[6] Similarly, capacity building and assistance between states presume subscription to the basic norm of cooperation.[7]

---

[3] A/70/174 (2015) para. 13 (a)–(k).

[4] Mika Kerttunen and Saskia Kiisel (eds), *Norms for International Peace and Security: The normative frameworks of international cyber cooperation*, (ICT For Peace Foundation, 2015), page 4.

[5] For different definitions of cooperation see William I. Zartman and Saadia Touval, *Introduction: return to the theories of cooperation*, in: William I. Zartman and Saadia Touval, *International Cooperation, The Extents and Limits of Multilateralism*, 2012, pages 1-12.

[6] A/70/174, para. 16; see also Mika Kerttunen and Saskia Kiisel (eds), *Norms for International Peace and Security: The normative frameworks of international cyber cooperation*, (ICT For Peace Foundation, 2015), page 6.

[7] A/70/174, para. 19-23.

4. Finally, recommendation (a) connects to the part on international law in the 2015 report. One of the international obligations emphasized with regard to the use of ICTs is the settlement of disputes by peaceful means under Articles 2 (3) and 33 (1) of the United Nations Charter.[8] Wherever two or more states find themselves faced with an international problem, it takes an act of cooperation to effectively examine and resolve it. This becomes evident considering the means for a peaceful settlement of disputes under Article 33 (1) of the United Nations Charter: negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice. The need for cooperation is shared among states as cooperation is one of the cornerstones of most national cybersecurity strategies.[9]

Background

5. Cooperation between states on an international level with regard to the topic of the use of ICTs can contribute to enhanced security and stability as it fosters common understandings and hence contributes towards predictability of behavior and transparency. In order to facilitate cooperation between states on the concrete topic of cooperation in the field of cyberspace, several cooperative platforms exist beside the United Nations.[10] The 2010[11] and 2013[12] reports list explicitly the African Union, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Asia Pacific Economic Cooperation Forum, the Council of Europe, the Economic Community of West African States, the European Union, the League of Arab States, the Organization of American States, the Organization for

[8] A/70/174, para. 26 and para. 28 (b).
[9] Contributions by Tang Lan and Mika Kerttunen.
[10] See also Mika Kerttunen and Saskia Kiisel (eds), *Norms for International Peace and Security: The normative frameworks of international cyber cooperation*, (ICT For Peace Foundation, 2015), page 6.
[11] A/65/201.
[12] A/68/98.

Security and Cooperation in Europe (OSCE) and the Shanghai Cooperation Organization.[13]

6. In addition to the United Nations Charter, general and particular expectations of cooperation flow from other international instruments such as the Friendly Relations Declaration.[14] In the declaration, states express their conviction that "states should cooperate in the economic, social and cultural fields as well as in the field of science and technology".[15] Principle (d) of the Declaration entails the "duty of states to co-operate with one another in accordance with the Charter."[16]

7. Furthermore, the Budapest Convention[17] entails provisions with regard to assistance as well as cooperation in the field of cybercrime. Art. 23 of the convention stipulates general principles with regard to international cooperation and art. 25 provides for general principles regarding mutual assistance. Such cooperation aims at combating cybercrime[18] and hence contributes to security and stability in the use of ICTs.

Expansion

8. The call for cooperation is one of those recommendations that some may consider already a binding obligation under international law. There are different arguments about the legal status of cooperation.

9. Some scholars emphasize, with reference to the Friendly Relations Declaration, the existence of a legal duty to cooperate, whereby cooperation would be understood as an obligation

---

[13] A/65/201, para. 13 and A/68/98, para. 14.

[14] United Nations General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 24 October 1970, A/RES/2625(XXV) (hereinafter: Friendly Relations Declaration).

[15] Ibid.

[16] Ibid.

[17] Council of Europe, Convention on Cybercrime, 23 November 2001 (ETS 185).

[18] Ibid., preambular para. 7.

to enter into coordinated actions.[19] The Friendly Relations Declaration establishes that states have the duty to cooperate with one another in accordance with the United Nations Charter. It has been argued that cooperation in the realm of the Friendly Relations Declaration can be defined as "voluntary coordinated action of two or more States which takes place under a legal regime and serves as specific objective".[20] Even though the Friendly Relations Declaration itself is not a legally binding agreement, it has been found to represent customary international law.[21] However, in the negotiations preceding the adoption of the Friendly Relations Declaration, representatives of several states stressed that this principle would not represent a legal but rather a moral duty towards state behaviour.[22]

10. It has also been argued that cooperation forms a general principle in international law[23] or a political-legal concept.[24] Furthermore, a duty to cooperate has been found to be the fundament of regimes dealing with shared resources.[25] The International Court of Justice states that a duty to cooperate exists as part of the International Convention for the Regulation of Whaling.[26] Also, the duty to cooperate has been emphasized

---

[19] Contribution by Kriangsak Kittichaisaree. See also Rüdiger Wolfrum, *International Law of Cooperation* (Max Planck Encyclopedia of Public International Law, 2010).

[20] Rüdiger Wolfrum, op. cit.

[21] For instance, see ICJ, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion, I.C.J. Reports 2010, p. 403, para. 80.

[22] Rüdiger Wolfrum, op. cit., para. 25.

[23] Christina Leb, *One step at a time: international law and the duty to cooperate in the management of shared water resources* (Water International, 2015, 40:1, pages 21-32).

[24] B. Babovic, *The Duty to Cooperate with One Another in Accordance with the Charter*, in: Milan Sahovic, (ed), *Principles of International Law Concerning Friendly Relations and Cooperation*, page 289.

[25] ICJ, Whaling in the Antarctic (Australia v. Japan: New Zealand intervening), judgment, ICJ reports 2014, page 226, Separate Opinion of Judge Ad Hoc Charlesworth, para. 13.; for examples of such regimes see Rüdiger Wolfrum, op.cit, para. 26 et seq.

[26] ICJ, Whaling in the Antarctic (Australia v. Japan: New Zealand intervening), judgment, ICJ reports 2014, page 226 para. 83.

in the regime on international environmental protection[27] and sustainable development in general.[28]

11. Considering those arguments, it remains subject to debate whether a general obligation of cooperation exists under international law.[29] However, international law allows a view whereby a duty to cooperate is not merely a voluntary and non-binding norm. In any case, the need for cooperation is obvious due to increasing interdependence of states in the context of use of ICTs. The modalities of such cooperation need to be established between and by states. In conclusion, this norm calls for cooperation between states and can therefore (at least in part) be considered a fundamental principle of interstate relations[30] because it emphasizes cooperative instead of unilateral actions.[31]

12. Regarding the emphasis of recommendation (a) on the development of cooperative measures in order to prevent threats against international peace and security, the argument could be made that the Friendly Relations Declaration imposes an obligation on states to this end, stating "states shall cooperate with other States in the maintenance of international peace and security". The concept of international peace and security relates to collective security measures vested with the United Nations Security Council.[32]

13. Traditionally, international peace and security has been closely linked to the use of military force and the notion of

---

[27] See principles 7, 9, 13, 14 of the *Rio Declaration on Environment and Development* (1992), United Nations Doc. A/CONF.151/26 (vol. I); art. 118 United Nations Convnetion of the Law of the Sea (UNCLOS); see also Rüdiger Wolfrum, op.cit, para. 28-37.

[28] See principle 5, 12, 27 of the Rio Declaration on Environment and Development (1992), United Nations Doc. A/CONF.151/26 (vol. I).

[29] Rüdiger Wolfrum, op.cit, para. 13-25.

[30] Contribution by Tang Lan.

[31] Contribution by Myriam Dunn Cavelty.

[32] Hitoshi Nasu, *The Expanded Conception of Security and International Law: Challenges to the UN Collective Security System* (VU University Amsterdam Vol 3:3, 2011), page 16.

armed aggression.[33] In this regard, international peace and security refers to the prohibition of the threat and use of force according to art. 2(4) of the United Nations Charter. Threat and use of force has generally been interpreted as meaning armed force including armed attack.[34] For considering if an act qualifies as an armed attack, the scale and effect of the act must be analysed.[35] It has been argued that if an attack results in physical damage,[36] such as death or injury to human beings or destruction or damage to objects, it can be considered an armed attack.[37] If considered an armed attack, it would also qualify as a use of force and therefore a threat to international peace and security.

14. However, today's threats to international peace and security are not necessarily limited to armed force.[38] Art. 39 of the United Nations Charter states that it lies within the powers of the United Nations Security Council to "determine the existence of any threat to the peace" and "to maintain or restore international peace and security." In this regard, the United Nations Security Council has acknowledged that also other sources in the "economic, social, humanitarian and ecological fields" can be considered threats to international peace and security.[39] Furthermore, the Security Council has, as of 2017,

---

[33] Karel C. Wellens, *The UN Security Council and New Threats to the Peace: Back to the future* (Journal of Conflict & Security Law 8:1, 2003), page 28.

[34] Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?* (Journal of Conflict & Security Law, 2012), page 216.

[35] ICJ, Case Concerning military and paramilitary activities in and against Nicaragua (Nivaragua v. United States of America) merits, judgment, ICJ Reports 1986, page 14.

[36] Russell Buchan, op. cit.

[37] Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, in: Christian Czosseck, Rain Ottis, Katharina Ziolkowski (eds), 4th International Conference on Cyber Conflict, (CCD COE, 2012) page 288. For further discussion of the concept of harm, see also commentary to recommendation (c).

[38] For an analysis of the Security Council determinations see for example René Värk, *Terrorism as a Threat to Peace* (Juridica International XVI/2009).

[39] "The absence of war and military conflicts amongst states does not in itself ensure international peace and security. The non-military sources

acknowledged cybersecurity as one focus point of protection efforts in the context of terrorist attacks against critical infrastructure.[40]

15. Recommendation (a) not only includes cooperation to prevent threats to international peace and security but also to prevent harmful ICT practices. With regard to the establishment of which ICT practices are considered harmful, Schmitt has argued that harm has to rise to such a level that it becomes "a legitimate concern in inter-state relations".[41] In the literature, harmful conduct has been considered within discussions on the applicability of a no-harm principle or due diligence obligation to cyberspace.[42] In this regard, it has been found that according to the existing sources of the principle, it only applies to physical damage;[43] malicious cyber activities might not cause physical damage but nevertheless be well perceptible such as a disruption of the stock exchange system.[44] The activities against Estonia in 2007 as well as millions of dollars in damages due to botnets are mentioned as examples for a classification of serious harmful consequences of ICT practices.[45] With regard to the target of malicious practices, the authors of the Tallinn Manual specify that, as long as the requirement of the severity threshold

---

of instability in the economic, social, humanitarian and ecological fields have become threats to peace and security", *Statement of the Members of the Security Council in the Note by the President of the Security Council* (United Nations S/23500, 31 January 1992). For a discussion regarding the concept of security in international law see Hitoshi Nasu, op. cit.

40 Security Council Resolution 2341 [on protection of critical infrastructure against terrorist acts], 13 February 2017 (S/RES/2341).

41 Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace* (125 Yale Law Journal Forum 68, 2015), page 76.

42 See for example Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013), page 30 et seq.; Jason Healey and Hanna Pitts, *Applying International Environmental Legal Norms to Cyber Statecraft* (A Journal of Law and Policy for the Information Society, 8:2, 2012); Katharina Ziolkowski, *General Principles of International Law as applicable in cyberspace*, in: Katharina Ziolkowski (ed), *Peacetime regime for state activities in cyberspace*, (CCD COE 2015).

43 See Katharina Ziolkowski, op. cit., page 166.

44 Katharina Ziolkowski, op. cit., page 163.

45 Jason Healey and Hanna Pitts, op. cit., page 379.

is met, it does not matter if the targeted infrastructure is private or governmental.[46] According to the Manual, a due diligence obligation only arises in the case that an act violates the right of a state and leads to serious adverse consequences.[47]

16. During the Sony incident in 2014, it was found that destructive malware was deployed in order to copy proprietary information and confidential information.[48] As a consequence, the FBI determined that the "actions were intended to inflict significant harm on a US business and suppress the right of American citizen to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior."[49] From this statement, it can be derived that the infliction of harm on businesses, hence economic harm, is seen as concern for interstate relations. The 2013 report itself mentions a broad notion of harm targeting "citizens, property and economy".[50] The phrasing of this part of the norm opens leeway for interpretation as no clear concept exists as to what is acknowledged to be harmful in the sphere of ICT practices.

17. Harmful interference in the realm of the Constitution of the International Telecommunications Union is closely connected to radiocommunication. In this regard, interference which interrupts radiocommunication and radionavigation services is considered harmful interference.[51] Therefore, art. 45 of the Constitution of the ITU obliges Member States not to use their radio stations to cause "harmful interference to the radio services or communications of other Member States." The Tallinn Manual acknowledges that the ITU regime and the provision on harmful interference is applicable to cyber

---

[46] Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the international law applicable to cyber operations* (Cambridge University Press, 2017), page 40, para. 36.

[47] Michael N. Schmitt and Liis Vihul, op. cit., pages 35-36, para. 21, 22.

[48] Update on Sony Investigation, FBI 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (25.11.2017).

[49] Update on Sony Investigation, FBI 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (25.11.2017).

[50] A/70/174, para. 7.

[51] CS/AN. 1003 Annex to the Constitution of the Inernational Telecommunication Union.

activities.[52] This is because cyber activities use radio waves which again rely on the eltromagnetic spectrum.[53] Besides this definition of harmful interference limited to radionavigation and communication, the Constitution specifies in Art. 42 the obligation that member states must not cause technical harm "to the operation of other telecommunication services of other Member States."[54] This provision can be seen as partially relating to the United Nations GGE recommendation.[55] Nevertheless, it is only concerned with technical harm to the functioning of services. This term connects to the notion of harmful interference. According to the Tallinn Manual, harmful interference from a technical perspective "occurs when two or more electromagnetic waves (…) overlap or partially or fully, thereby degrading or cancelling each other."[56] It could therefore include unintentional harm.[57] Nevertheless, the term harm might be interpreted more broadly as introduced in the following paragraphs. The proposal to rephrase art. 6 of the International Telecommunication Regulations (ITR) to also include the notion of maintenance of international peace and security,[58] might be regarded as an extension of the ITU's competences and should therefore be considered carefully.

18. With regard to the above-mentioned considerations, the question arises as to what damage passes the threshold of being acknowledged to be harmful. The 2010 report expresses concern towards practices, which damage information resources and infrastructures.[59] The 2015 report then explicitly refers to attacks using ICTs that are targeted against critical infrastructure and

---

[52] Michael N. Schmitt and Liis Vihul, op. cit., page 296, para. 6.
[53] CS/AN. 1005, Note 1, Annex to the Constitution of the International Telecommunication Union; see also Michael N. Schmitt and Liis Vihul, op. cit., page 295, para. 2.
[54] See also art. 1.169 ITU Radio Regulations (2016).
[55] See Richard Hill's contribution to this commentary, page 1.
[56] Michael N. Schmitt and Liis Vihul, op. cit., page 296, para. 7, footnote 728.
[57] Michael N. Schmitt and Liis Vihul, op. cit., page 295, para. 5.
[58] Contribution by Richard Hill, page 2.
[59] A/65/201, para. 4, 6.

associated information systems as "the most harmful attacks".[60] The threat of attacking critical infrastructure is also stressed by countries' contribution to the GGE.[61] Concern is furthermore expressed towards harm caused to citizens, property and economy.[62] This does not only include activities carried out by states but explicitly entails criminal acts.[63] Therefore, the elements of offense as included in the Budapest Convention can give guidance on which practices are considered to be harmful when it comes to criminal activities carried out through the use of ICTs. Art. 2-10 of the Budapest Convention include illegal access to computer systems, interception without right, data interference, system interference, misuse of devices, forgery and fraud through the use of computer data, offences related to child pornography and infringements of copyrights. Serious damage to the economy, national and international security would be perceived as harmful by the international community.[64] Furthermore, targets of such harmful conduct would include individuals and legal entities, national infrastructure and governments, public safety, state security and stability of the international community as a whole.[65]

19. Germany, Greece and the United Kingdom also stress the importance of protection of availability, integrity and confidentiality of data and hence the protection of communication.[66] Therefore, the theft or destruction of digital data would be considered harmful.[67] Switzerland considers

---

[60] A/70/174, para. 5.

[61] See submissions of Estonia, Germany, Singapore, Qatar, UK to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[62] A/70/174, para. 7.

[63] A/65/201, para. 5.

[64] Contribution by Anatoly A. Streltsov, page 9, para. 3.

[65] Ibid.

[66] Submissions of Greece and Germany, UK to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[67] Submissions of Greece to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

cybercrime, espionage and sabotage as harmful conduct.[68] Singapore mentions the danger of harm to the function of CERTs. Collective action of states is also demanded by art. 6 of the ITR,[69] in order to prevent harm to the international telecommunication networks.[70] However, some states refused to sign the ITRs due to the concern that this article could be used to justify violations of the freedom of speech.[71] Concluding, it can be argued that, due to the steadily evolving technological capabilities as well as the non-existing communication by governments with regard to their stance towards certain ICT practices, it is difficult to point out an established threshold for harmful ICT practices.

Analysis

20. States that issued a national cybersecurity strategy acknowledge cooperation as one of the main principles in combating emerging threats.[72] Additionally, all states emphasize the necessity of cooperation with regard to threats emerging due to the use of ICTs in their national contributions to the GGE in 2017.[73] Wingfield observes that cooperation can take place in different fora focusing on regional, bilateral, multilateral, like-minded states or cooperation between states with contrary or largely different interests.[74] Different forms of cooperation have different advantages and disadvantages. For instance, diverse geographical representation can be of advantage for achieving broad agreement

---

[68] Submission of Switzerland to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[69] Art. 6 ITR 2012: "Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public."

[70] Contribution by Richard Hill, page 2.

[71] Ibid.

[72] Contribution by Mika Kerttunen.

[73] A/72/315.

[74] Contribution by Thomas C. Wingfield.

while, at the same time, negotiating with like-minded states could be more promising in terms of reaching a binding agreement.[75] In this regard, the explicit need for alternative fora besides the United Nations has been stressed because the negotiations within the United Nations are deemed insufficient.[76]

21. Examples of agreements between like-minded states are the Budapest Convention on Cybercrime as well as the agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security. Other cooperative measures such as discussions, program trainings and exercises are carried out in the realm of the Commonwealth of Independent States (CIS).[77] Further cooperation between like-minded states takes place within regional organizations such as the OSCE, the North Atlantic Treaty Organization (NATO), the Council of Europe, the South American Common Market or the Organization of American States, and el congreso y Feria Iboamericana de Seguridad de la Información. Other fora in which cooperation in the field of cyberspace takes place is the Collective Security Treaty Organization, the European Union and NATO.[78]

22. Multilateral cooperation focusing on the inclusion of a broader range of states takes place at the level of the International Telecommunication Union as well as the GGE. An example of bilateral cooperation is the Canada–United States Cyber Security Action Plan, the United States–Canada Electric Grid Security and Resilience Strategy.[79] Also Germany, Japan and Norway emphasize the need for bilateral cooperation.[80]

---

[75] Contribution by Microsoft, page 4.

[76] Ibid., page 1.

[77] See submission of Armenia to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[78] Ibid.

[79] Submission of Canada to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[80] Submission of Germany to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

23. States and scholars have different views as to which threats should be prioritized in the context of prevention and mitigation. For example, the United States emphasizes security of critical infrastructure[81] and hence would consider threats against them as not tolerable. China, on the other hand, stresses the importance of regulating access to information.[82] Belarus has emphasized the danger of attacks against critical infrastructure and information technology infrastructure such as power plants and systems to provide production and transport.[83] Brunei Darussalam defines hacking, cybercrimes and cyberterrorism targeting vital infrastructure, networks and services as threats in cyberspace.[84] Generally, cyberattacks and cyber espionage have been mentioned to be acknowledged to be harmful.[85] Cuba considers acts directed to disrupt the judicial or political order as threats to international peace and security.[86] In this respect, specific activities threatening this order are foreign radial and television transmissions.[87] Ecuador emphasizes that espionage of citizen's communications and related interference into the internal affairs of states infringing sovereignty under international law represent a threat to international peace and security.[88] Furthermore, it has been argued that concepts of threat and harm focus on cyberattacks with disruptive effects.[89]

---

[81] Contribution by M. A. Gomez.

[82] Ibid.

[83] Submission of Belarus to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[84] Submission of Brunei Darussalam to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[85] See Kriangsak Kittichaisaree's contribution to this commentary.

[86] Submission from Cuba to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[87] Submission of Cuba to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[88] Submission of Ecuador to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[89] Contribution by Myriam Dunn Cavelty.

In this regard, mega-hacks and advanced persistent threats are signs for the maturity of cyberattacks.[90] However, one view is that activities that are not destructive such as the extraction of data would not be considered harmful or a threat to international peace and security.[91] Accordingly, it becomes a requirement for states, in their implementation of recommendation (a), to determine and specify their respective priorities and criteria on what they consider as harmful and threatening in the context of the development and uses of ICTs.

24. With respect to various threats, the GGE offers several practical ways of cooperation. Several states have emphasized the value of confidence-building measures (CBMs) with regard to strengthening trust and contributing to stability and security in cyberspace.[92] Para. 17 of the 2015 report outlines possible cooperative measures pertaining to detection and mitigation of ICT incidents. Canada has additionally emphasized the utility of CBMs introduced by the OSCE, for the purpose of international cybersecurity. The OSCE CBMs, for example, include information sharing on national organizations, expert's meetings, communication and cooperation amongst CERTs as well as mitigation of attacks targeting critical infrastructure.[93] The 2016 OSCE CBMs focus explicitly on cooperation between states by including measures aimed at the mitigation of attacks on critical infrastructure, which could affect more than one state.[94]

25. According to para. 10 of the Annex to United Nations General Assembly Res. 58/199 (2003) cooperation may consist in "developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks

---

[90] Ibid.

[91] Ibid.

[92] See submissions of Finland, Germany, Japan, Jordan, Portugal, Switzerland, UK, available online: https://www.un.org/disarmament/topics/informationsecurity/.

[93] Submission of Canada to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/; see also OSCE, Decision No. 1202, PC.DEC/1202 (2016).

[94] OSCE, op. cit., para. 16.

on such infrastructures in accordance with domestic laws."[95] However, it has been argued that at the same time, states engage in activities damaging trust and confidence. Those activities include the strategic exploitation of vulnerabilities in computer systems as well as weakening encryption standards.[96]

26. Capacity building and cooperation between economically developing and developed states is important for reaching agreement between those countries regarding Internet governance. In this respect, the divide between signatories and non-signatories of the 2012 Telecommunications Regulation shows the need for enhanced cooperation.[97] To strengthen interstate cooperation, the transfer of information technologies to developing countries is considered to be a measure to combat "the criminal use of information technology".[98] The assistance of economically developed countries as a form of capacity building and cooperative measures was stressed by Afghanistan's 2017 contribution to the GGE. Afghanistan emphasizes in this regard especially vocational and technical training. Similarly, Brunei Darussalam stresses cooperation in the realm of ASEAN in order to enhance capacity building, which itself contributes to the protection of cyberspace.[99] As an economically developed country, Canada has developed Anti-Crime and Counter-Terrorism Capacity Building Programs; Canada supports in this regard the Organization of American States and in equipping and training of ASEAN countries in the field of cybersecurity and cybercrime.[100] Similarly, Japan

---

[95] *Creation of a global culture of cybersecurity and the protection of critical information infrastructure*, Resolution 58/199 of 2003 (A/RES/58/199). See also Annex C United Nations General Assembly Res. 57/239 (2003).

[96] Contribution by Myriam Dunn Cavelty.

[97] Richard Hill, *Dealing with Cyber Security Threats: International Cooperation*, *ITU, and WCIT*, in: Maybaum, M., Anna-Maria Osula, Lauri Lindstöm (eds), 7th International Conference on Cyber Conflict (CCD COE 2015), page 126.

[98] A/RES/58/199.

[99] Submission of Brunei Darussalam to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[100] Submission of Canada to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

acknowledges its commitment to capacity building.[101] Finland is founding partner of the Global Forum on Cyber Expertise, a platform for the exchange of expertise and capacity building.[102] Additionally, Finland joined the World Bank's Digital Development Partnership Trust Fund.[103] Further countries such as Germany, the Netherlands, Portugal, Singapore, Switzerland and the United Kingdom are committed to capacity building programs as they express in their respective contributions to the 2017 GGE.

Recommendations

- States should acknowledge the principle of cooperation as fundamental to the maintenance of international peace and security.
- States should specify and determine modalities of cooperation in line with their particular views on which ICT practices are harmful or constitute a threat to international peace and security.
- In order to clarify their goals and priorities in cyberspace, states should develop or upgrade national cybersecurity strategies and domestic policies.
- States should be guided by the United Nations GGE, OSCE and other relevant processes' recommendations as to the practical measures of cooperation.
- States, in their cooperation, should consider the role of their industry, academia and civil society when specifying and implementing the modalities of cooperation.

---

[101] Submission of Japan to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[102] Submission of Finland to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

[103] Submission of Finland to the United Nations Secretary-General's report (A/72/315), available online: https://www.un.org/disarmament/topics/informationsecurity/.

Recommendation 13 (b)

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.

Mika Kerttunen

Contextualization

1. Recommendation 13 (b) primarily addresses the issue and concern of State responsibility and the prevention of conflicts and the risk of escalation during and due to a cyber incident. An originalist reading of the recommendation emphasizes the inflicted State's cautious behavior during an ICT incident. Yet, it is tempting to interpret the recommendation to facilitate measures to support such considerations, assessments as well as international attribution.

2. As such the recommendation is ideationally linked, but without explicit reference in the GGE reports, to the general principle and norm of peaceful settlement of international disputes without endangering international peace, security, and justice.[1] More specifically the recommendation is linked to the notion of disruptive activities criminals, terrorists and States themselves may conduct, as outlined in the 2010 United Nations GGE report.[2] Despite the fact that the notion of consequences

[1] The United Nations, Charter of the United Nations, Article 2(3).
[2] A/65/201, para. 1, 4-8.

is included in recommendation (b), it does not address doctrine of consequences or State right to respond to ICT perpetrators. The recommendation refers to and underlines the need to consider the nature and extent of consequences of the (very) ICT incident. The nature and extent of these consequences under international, and national, law play a role in determining political, legal and financial responsibilities and measures.[3]

3. The 2010 report itself does not go to elaborate any norm (or rule or principle) but recommends examining the need for cooperative actions and mechanisms and hints of the need of "additional norms" that could be developed over time.

4. In the 2013 report, the discourse of conflict prevention and attribution continued and deepened. It noted the State interest in preventing conflicts arising from the use of ICTs, a statement that presumes the use of ICTs causing such a risk. Moreover the report raised the difficulty of attribution to a specific perpetrator, and noted how the development and the spread of sophisticated malicious tools and techniques may further increase the risk of mistaken attribution and unintended escalation. In this respect, among cooperative measures to enhance international peace, stability and security, the application of relevant international law and derived norms, rules and principles of responsible behaviour of States were mentioned.[4]

5. The norms, rules and principles the 2013 GGE report recommended did not directly address the issue of attribution or other national incident management mechanisms. The most direct reflections in this respect can be found in the section (IV) on "Recommendations on confidence building measures and the exchange of information". The Group recommended enhanced sharing of information among States on ICT security incidents,

---

[3] The nature and extent of ICT incidents related to International Humanitarian Law and to the notions of use of force and armed attack are under political and schorly discussions. Such linkages remain disputed.

[4] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98), para. 4-6, 11.

including "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".[5] These measures and practices if instigated would form an institutional and cognitive foundation for conflict prevention and further norms-guided State behaviour. The section (V) on "capacity-building measures" recommended, inter alia, increasing "cooperation and transfer of knowledge and technology for managing ICT security incidents".[6]

6. The 2015 report reiterated the risks and threats in the use of ICTs as well as the difficulty of attribution but also lifted up the concern of the danger of destabilizing misperceptions. The Group listed eleven items as "recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment", including the recommendation in question.[7]

7. The 2015 report explicitly took up the issue of attribution in the section (VI) on international law applying to the use of ICTs. The Group referred to States obligations regarding internationally wrongful acts attributable to them under international law, and noted that "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State". Moreover the Group specifically noted that "the accusations of organizing and implementing wrongful acts brought against States should be substantiated", a demand that directly flows from recommendation (b).[8]

---

[5] Ibid., para. 26c.

[6] Ibid., para. 32d.

[7] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174), para. 7, 13.

[8] Ibid., para. 28f.

Background

8. The issues of attribution, State responsibility and responses that recommendation (b) carries were born against the backdrop of events, doctrinal development and normative moves that had, in the early 2010's, created anticipation and fear of proliferating political use of cyber means. This climate of fear and operational success conditioned the above-elaborated normative development and the genealogy of norm 13 (b).

9. The cyber attacks against Estonia in 2007 brought the issue and challenge of attribution to general awareness—and of significance to international relations. Despite the attacks emanating from computers in 178 countries, some attackers were identified by their IP addresses, including a few cases where the IP address involved in the attack belonged to Russian state institutions. Political attribution was apparently claimed in March 2009 when a State Duma Deputy of the pro-Government Unified Russia party stated that the Estonian attacks had been carried out by his assistant as part of "a reaction from civil society".[9] Yet the political context, some IP addresses and a politically motivated statement were not sufficiently strong evidence.

10. The *Stuxnet* malware discovered in January 2010 in an Iranian nuclear enrichment facility, the 2012 *Shamoon* cyber attacks against Saudi Aramco as well as the 2013 attacks against United States banks are other examples of the challenged and multifaceted nature of attribution. The malware and the attacks are contextually interlinked based on series of assumptions and deduction: that the United States and Israel, in their effort to slow and stop Iran's nuclear endeavours, were behind *Stuxnet*, and that Iran, as response and reprisal, had launched the subsequent attacks.[10] The assumed and accused State parties have either denied their involvement or refused to comment.

---

[9] Eneken Tikk, Kadri Kaska and Liis Vihul, International Cyber Incidents. Legal Considerations (Tallinn: CCDCOE, 2010), page 23-24.

[10] The professional, academic and popular literature on Stuxnet is vast. For a contextualizing analysis that links Stuxnet and Shamoon see e.g.

11. Particularly in the United States, attribution and accusations of cyber attacks and network exploitation have been made to countries such as China and the Democratic People's Republic of Korea. For example, the influential Washington-based think tank Center for Strategic and International Studies (CSIS) published in March 2013 a report listing open sources that associated Chinese governmental organs as well as individuals to cyber incidences.[11]

12. What is common to the above-mentioned cases, as many others, is that at least publicly available evidence on attribution is often circumstantial or based on previously identified characteristics, such as known techniques, handwriting and embedded scriptures. Most importantly cyber incidents and attribution tend to correlate with real-world tensions, again underlining the linkage between the politics and procedures online and off-line, as well as the virtual and the physical world.

13. These and other such examples of incidents highlight the core issues of recommendation (b), attribution of responsibility for the incident to a state with an intent to define a subject of international law to which international legal responsibility in connection with the incident can be applied.

14. The way the highest United States intelligence and security directors explained in October 2016 the alleged Russian responsibility of the Democratic National Committee testifies not to the challenges of technical attribution but to the near impossibility of certainty in political attribution.

15. Three United States official documents signify the anticipation of success to conduct cyberspace operations and attribute attacks to their origins. The 2011 United States *International Strategy for Cyberspace* reserved the right to use all necessary means as response to hostile acts in cyberspace; moreover the *International Strategy* also stated that the United States "will take measures to identify and respond to

---

Christopher Bronck and Eneken Tikk-Ringas, *Cyber Attacks against Saudi Aramco* (Survival: Global Politics and Strategy, 55:2, 2013).

[11] Laura Saporito and James Lewis, *Cyber Incidents Attributed to China* (CSIS, March 2013).

such actions to help build an international environment that recognizes such acts as unlawful and impermissible, and hold such actors accountable".[12] The leaked/stolen 2012 Presidential Policy Directive *U.S. Cyber Operations Policy* (PPD-20) followed the *International Strategy* and described the integration of defensive and offensive cyber operations with other policy tools and options. When taking action, effectiveness, costs, risks, potential consequences, foreign policy, and other policy consideration were to be taken into account.[13] The 2013 military doctrine *Cyberspace Operations* (JP 3-12 (R)) notices the difficulty of attribution but focuses on the joint level planning and conduct of cyberspace operations.[14]

16. On the normative front, in particular, the *Tallinn Manual on the International Law Applicable to Cyber Warfare*[15] supported the interpretation that cyber activities are attributable to State and, given their scale and effects, can constitute use of force and armed attack. On the other hand, Russia and China, together with their Central Asian partners, jointly submitted a proposal on an international code of conduct for information security.[16] The *Code of Conduct* speaks of the importance of international legal norms and the role of international organizations. Directly relevant to the norm is the mentioned need to reduce the likelihood of misunderstanding and the risk

---

[12] The White House, *International Strategy for Cyberspace* (May 2011), pages 14 and 18.

[13] The White House, *U.S. Cyber Operations Policy*, PPD-20 (16 October 2012). Published by The Guardian on 7 June, 2013.

[14] Joint Chiefs of Staff, *Cyberspace Operations* (Joint Publication No. 3-12 (R), 5 February, 2013), pages I-7 and II-9. Consequently, a 2017 Department of Defence report on cyber deterrence emphasises the need to accelerate the improvement of cyber attribution capabilities (Defence Science Board, Task Force on Cyber Deterrence (February 2017).

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

[16] 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 of 13 January 2015). The first version of the Code of Conduct was submitted in 2011 (A/66/359).

of conflict. The 2015 BRICS Ufa Declaration announced expert-level cooperation in, among others, sharing of information and best practices relating to security in the use of ICTs, capacity building and the development of international norms, principles and standards.[17]

17. Finally, in portraying the politico-normative landscape of the first half of the 2010's, it should be noted that the 2014-2015 GGE itself referred to the "inherent right of States to take measures consistent with international law", as well as to the "principles of humanity, necessity, proportionality and distinction",[18] yet, without reference to International Humanitarian Law, their origin. These moves can be interpreted to open the discussion on the right of self- or collective defence.

Expansion

18. Extensive amount of literature discuss the individual elements and capabilities that the recommendation contains, in particular situational awareness, digital forensics, information sharing, attribution, and the nature and extent of cyber incidents.[19] Alongside such practically oriented literature politico-normative discourse has been focusing on State behaviour, the concrete action before, during and after cyber incidents.

19. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* notes that technical attribution remains challenging but possible from a legal-normative perspective and for political purposes. The key normative question in attribution is responsibility of action, that is incidents and operations. The *Manual* draws its guidance from the International Law Commission's 2001 "Draft Articles on Responsibility of States for International Wrongful Acts", and states that "under international law, States may be responsible for cyber operations that their organs conduct or

[17] VII BRICS Summit, Ufa Declaration (17 June 2015), para. 34.
[18] A/70/174, para. 28c and 28d.
[19] This body of literature remains outside of this examination.

that are otherwise attributable to them by virtue of the law of State responsibility. The actions of non-State actors may also sometimes be attributable to States".[20] This recognition has dual significance: it elevates cyber operations to the conceptual and legal level as any other State activity and it reinforces the State–non-State actor connection.

20. Of the latter, the *Manual* emphasises that attribution only occurs when the entity in question is acting in the empowered capacity. The conditions are that the acts are of governmental character and the entity is empowered by the State to carry out such acts. Therefore, as the *Manual* later continues each situation need to be assessed in context.[21]

21. Another central question in attribution are the modalities of attributing non-State actors' conduct to a State. As the International Court of Justice has outlined, the underlying criteria is effective control a State has exercised over non-State actor operations. The *Manual* maintains the doctrine of control but points out that State activities, e.g. in supporting non-State actors, may constitute a violation of international law without such attribution of their operations to a State.[22]

22. On the issue of attribution, the International Group of Experts behind the *Tallinn Manual 2.0* had considered the issue of a State bearing an obligation to publicly provide evidence of attributing *cyber operations* to another State. They concluded that, although it "may be prudent" to do so, there is no sufficient State practise and *opinio juris*, and thus established basis to conclude that such an obligation exists under international law.[23] In this question, the United States for example has maintained the similar position that "there is no international

---

[20] Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), p. 15.

[21] Michael N. Schmitt, op. cit., pages 90-92.

[22] Michael N. Schmitt, op. cit., pages 94-100.

[23] Michael N. Schmitt, op. cit., page 83. On attribution and State responsibility, see also Kriangsak Kittichaisaree, Public International Law of Cyberspace (Cham: Springer, 2017), pages 32-44.

legal obligation to reveal evidence on which attribution is based prior to taking appropriate action".[24]

23. One of the most disputed conclusions of the *Tallinn Manual* is the claim that a "cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force"; the similar logic and criteria is applied to the question of armed attack. These conclusions are anchored to the doctrine of effects and consequences constituting the criteria and are in line with the International Court of Justice *Nicaragua* judgment where scale and effects are to be considered when determining actions amounting to an armed attack.[25] As Schmitt had observed already in 1999, "the international community is not directly concerned with the particular coercive instrumentality used (force in this case), but rather the consequences of its use".[26] Neither target nor means are considered sufficient to determine when the thresholds of use of force and armed attack are crossed. It should be noted that the United States maintains the view that there are no two thresholds; on the contrary, keeping use of force and armed attack apart is seen to create a dangerous zone of ambiguity that allows harmful and malicious activities.

Analysis

24. Unanimously, commentators of recommendation (b) defined the core of the recommendation being avoiding unnecessary escalation among countries. They pointed out that the purpose of attribution, tracking attackers, is to determine

---

[24] Brian Egan, *International Law and Stability in Cyberspace* (2016), page 19.

[25] Michael N. Schmitt, op. cit., Rule 69 (Use of Force), Rule 71 (Armed Attack), pages 330 and 339. These conclusions were already drawn (Rule 11; Rule 13) in Michael N. Schmitt (ed.) (2013), op. cit.

[26] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (The Columbia Journal of Transnational Law, Volume 37, 1999).

responsibility and subsequent punishment.[27] It was also highlighted that an ICT incident can affect both cyberspace and the media sphere, in the former affecting the functionality of the technical components and in the latter violating the confidentiality of information, violation of freedom of speech and expression of thought as well as the abuse of this freedom. Moreover it was observed that the notion of international incident in the ICT sphere is defined, above all, by the nature of international relations between the states affected by the incident caused mainly by unforeseen government actions but also by agents of one state against another state.[28]

25. The assessment of nature and scope of consequences of an ICT incident as well as attribution of responsibility for the incident to a state were seen as an intention to define a subject of international law to which international legal responsibility in connection with the incident can be applied. As one commentator explained:

> These consequences provide duty of a subject of international law to eliminate damage caused by it to another subject of international law through the breach of legal international obligation, or obligation to compensate material damage caused by actions that do not violate norms of international law, if such compensation is stipulated by a special international treaty.[29]

26. Another commentator however raised three comments: firstly, that non-State actors can also cause incidents; secondly, emphasizing that, instead of international legal norms or norms of international law, it is more accurate to speak of international obligations or international legal rules; and, finally, that the duty of a subject of international law is to cease the breach of the obligation as well as that the compensation may not be dependent on the provision of a special treaty.[30] This set

---

[27] For example, Anatoly A. Streltsov's and Tang Lan's contributions to this commentary.

[28] Anatoly A. Streltsov's contribution to this commentary.

[29] Anatoly A. Streltsov's contribution to this commentary.

[30] Nohyoung Park's contribution to this commentary.

of comments already reflects the division of position among the countries who have participated in the GGE process, in particular the 2016-2017 session: to what extent international obligations actually obligate States, and does international law contain sufficient regulations or is *lex specialis* needed.

27. One commentator explained the ICT sphere as a space where rules, principles and regulations are to a large extent not covered by international treaties but are featured as international legal custom. Therefore, as international custom serves as the basic and, "in fact", in this case, the only source of the law of international responsibility, its use is difficult.[31]

28. On the issue of attribution, it was noted that, as a general rule of international responsibility, a State is responsible for acts of all its bodies and of officials, but it cannot be attributed responsibility for behavior of individuals. It however can be considered internationally responsible for its actions in connection with actions of individuals. Furthermore, presuming credibility of injured state law enforcement and investigating bodies was implicitly questioned. Consequently, some commentators were unified in presuming confidence in a third party, for example an authorized international organization for attribution.[32] As noted above unilateral public attribution seemed easily to appear as politically motivated and eroding "the mutual trust while less benefit to deal with the event".

29. A universal approach to attribution was considered for further examination: at the international level, deliberating the feasibility of building an organization under the United Nations Security Council that would consist of two affiliations taking charge of technical attribution, and political and legal responsibility contribution, respectively. The *Global Consortium for Cyber Attribution* that RAND and Microsoft have initiated

[31] Anatoly A. Streltsov's contribution to this commentary.

[32] Anatoly A. Streltsov's, Nohyoung Park's and Microsoft's contributions to this commentary. Streltsov continued to list techniques of peaceful settlement of international disputes-negotiation, inquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional bodies or other peaceful means at one's own option-as useful means to solve the challenges of attribution. Park added fact-finding to the list.

could accordingly "act as one affiliation to provide independent technology attributing details and conclusion, build the foundation for political decision". It was considered essential that the international attribution organization needs to provide an appealing channel for victims of major cyber attacks. Despite the recognized shortcomings of the United Nations system, the constitution and function, even the possibility of this organization to be put on the agenda, were called for. Secondly at national level, effective communicating channels among countries, especially in the time of crisis are needed as the first step of risk management standard procedure to help reduce misperception to some extent.[33] On the issue of international attribution embedded or stemming from recommendation (b) under review, it was however noted that the recommendation does not imply to international bodies or attribution.[34]

30. Yet an explicit recommendation to establish an attribution organization was forwarded. Investigating how such an organization could be established and operate was seen to improve accountability and adherence to cybersecurity norms:

> Ultimately, however, the success of cybersecurity norms depends on whether they are implemented faithfully and whether violators are held accountable. The ability to assign responsibility is the linchpin of accountability.[35]

31. It was also noted how many of the concepts involved remain undefined, misunderstood and causing problems to grasp what is meant and how to apply a particular norm. This ambiguity around the terminology was seen to allow "states to continue to act in violation of established norms, without the international community having recourse to respond".[36]

32. Moreover, to improve the implementation of the recommendation, one commentator suggested it to be added

---

[33] Tang Lan's contributions to this commentary.
[34] Nohyoung Park's contributions to this commentary.
[35] Microsoft's contribution to this commentary.
[36] Ibid.

as an additional provision for article 6 of the International Telecommunication Regulations as such.[37]

33. Two statements help summarize the concerns some commentators expressed: that the purpose of recommendation (b) is to reduce risk of international disputes or conflicts through binding obligations on a state to examine all the relevant information in case of an ICT incident:

> Basically, we are talking about development of certain international procedural norms governing enforcement activities of actors of international law in investigation of incidents in the ICT sphere.[38]

and finally:

> [w]e have already seen examples of tit-for-tat attacks, and without a clear understanding what behavior is permitted, conflict—first online and then kinetic—can easily be the result.[39]

34. As the prevailing conventions the leading States differ, universal adherence to the recommendation is difficult. For example, the inclusion of media sphere and freedom of information within the scope of the recommendation is alien to western thinking. It nevertheless highlights a key difference between national approaches and preferences. For some, the issue is of information control, information security and information operations, for others freedom of information, cybersecurity and cyber operations; the countries are ideologically divided in this area that many still regard to be mainly technical. The semantics matter because they contain political and administrative connotations and practises and, as commented, ambiguities can allow, even trigger, violation of norms and deny victim State responses.

35. The recommendation *an sich* does not address any single threat or threat actor but is more generally of State behaviour in an environment of "dramatic increase in incidents involving

---

[37] Richard Hill's contribution to this commentary.
[38] Anatoly A. Streltsov's contribution to this commentary.
[39] Microsoft's contribution to this commentary.

the malicious use of ICTs by State and non-State actors" and the trends that "create risks for all States, and the misuse of ICTs" that "may harm international peace and security" as portrayed in the United Nations GGE 2015 report. Essentially relevant is the experts' notice of the danger of destabilizing misperceptions that "the States are rightfully concerned about".[40]

36. Even more challenging is to find agreement on the question of cyber activities constituting or not constituting use of force or armed attack. As noted above, the permissive interpretations acknowledge the Draft Articles of the International Law Commission or the custom they reflect, but a restrictive reading of International Law does not recognize the Commission's authority to create International Law; thus, without such constitution, there is not or cannot be any right to countermeasures or self- or collective defence in this respect.

37. Recommendation (b) permits four widening interpretations not alien to politico-normative speech: the recommendation in its absolutism denies ever justifiably attributing an incident to a State; the demand of context overrides the act itself and points to circumstances where cyber means are or are not justifiably used; the challenges of attribution call for more potent international attribution; and the nature and extent of a cyber incident can align with the criteria of use of force or armed attack to justify the victim State's or its allies' right to respond.

38. This interpretative meaning-giving, albeit logical, however, stretches the recommendation into something unrecognizable. Rather than deriving for (the existing) international law these interpretations wish to redefine it. Admittedly, the purpose of the recommendation can be used to determine its scope and application, but, in a situation where there is no normative-legislative or interpretative history to offer guidance, textual reading is the only plausible way to approximate the recommendation. The recommendation does not deny attribution, it does not call for an international organ, and it does not speak of rights of countermeasures or facilitate self- or collective defence. The recommendation purely offers

[40] A/70/174, para. 3 and 8.

procedural guidance and, given its context, to prevent conflict or reduce risk of escalation. Such escalation could easily take place in the opposite, negative situation where coincidental information affects considerations, the challenges of attribution are overlooked, the wider context is forgotten or the nature and extent of the incident do not matter in determining State behaviour. By its procedural guidance, it is appropriate to claim that the recommendation speaks of prudence. For the afore-elaborated political and practical discourses and the other, often more particular, recommendations, recommendation (b) serves as a preamble, being even close *jus cogens*.

39. An issue that the commentators did not raise, but which should be examined, is the very notion of "all relevant information" the recommendation centres on. Two issues command attention, firstly the relevance of information itself and secondly the demands of acquiring and considering all and relevant information.

40. The relevance of information is a question of evidence: what constitutes relevant, necessary and sufficient evidence to define a subject of international law to which international legal responsibility can be applied? There is no universal or interdisciplinary agreed concept of evidence. On one hand Thayer holds an influential view that relevance "is an affair of logic and not of law", that "the law furnishes no test of relevancy";[41] on the other hand, there are several attempts to establish legal standards of proof, which then are often based on logical reasoning or mathematical probability.[42]

---

[41] James Bradley Thayer, *A Preliminary Treatise on Evidence at the Common Law* (Boston: Little, Brown, 1898), pages 265-269. That Thayer speaks of the common law underlines the challenge of proof, relevancy and evidence within international law—and cyber affairs.

[42] On the issue of evidence see for example, Ronald J. Allen and Michael S. Pardo, *The Problematic Value of Mathematical Models of Evidence* (Journal of Legal Studies, 36, 2007); and on evidence in international cases e.g. Mary Ellen O'Connell, *Rules of Evidence for the Use of Force in International Law 's New Era* (Notre Dame Law School, Scholarly Works, paper 35, 2006).

41. National cybersecurity documents are not keen to examine the issue of evidence. The defence, deterrence and law enforcement emphasising the 2016 United Kingdom cybersecurity strategy goes to inform that the Goverment programmes and evidence-based policies will include, inter alia, "all-source assessment and other available evidence" and take into account "assessments from all available sources".[43] These references do not explicitly refer to attribution or State responsibility by international law, but, most importantly for this study, describe and guide national procedures. On the other hand the 2017 United States House of Representatives Bill proposal "Active Cyber Defense Certainty Act" takes the relevance and weight of evidence for granted when it merely speaks of notification for the use of active cyber defence measures:

> Notification must include the type of cyber breach that the person or entity was a victim of, the intended target of the active cyber defense measure, the steps the defender plans to take to preserve evidence of the attacker's criminal cyber intrusion, as well as the steps they plan to prevent damage to intermediary computers not under the ownership of the attacker and other information requested by the FBI to assist with oversight.[44]

42. The received commentary opens up the question of determining authority of attribution and applying State

---

[43] HM Government, *National Cyber Security Strategy 2016-2021* (November 2016), para. 7.2.4 and 7.4.5. The 2016 Australian strategy speaks of evidence based investment decisions (Australian Government, *Australia's Cyber Security Strategy*, April 2016), page 25.

[44] *Active Cyber Defense Certainty Act*, H.R.4036, 115th Congress (2017-2018) (12 October 2017), Section 5:2. Section 6(b) describes a "voluntary preemptive review" process the FBI and other agencies to "review the notification and provide its assessment on how the proposed active defense measure may be amended to better conform to Federal law, the terms of section 4, and improve the technical operation of the measure". The Bill is to "amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes".

responsibility. The cited House proposal wants to offer keys to private persons. Victim State truthfulness and competence has already been questioned. Doubts can be cast on the International Court of Justice and the United Nations Security Council's ability, too. The ICJ recognizing the difficulty of collecting classified evidence has been observed to take more liberal view to inferences of fact and circumstantial, and rebuttable, evidence. The United Nations Security Council then is a body of political decision-making where the standards and burden of proof being flexible can fluctuate.[45]

43. The impossibility of finding and agreeing upon sufficient, weighty, evidence will not disappear in the case of an international agency either. It is likely that by performing fact-finding to ascertain where the truth lies, such 'an attribution council' would land amidst political quagmire of endless disputes on the nature and quality of facts and its work. In fact the political problems of cyber incidents in general and victim State responses in specific would be reduced to technocratic debating.

44. Secondly, the recommendation assumes national capacity without which it cannot be followed. It can only be implemented with sufficient national cognitive, organizational and technical capabilities. The recommendation thus sets additional demand to developing countries. In fact, any behavioural assessment of adherence to the norm would inevitably also become an assessment of capacity.

45. In short and in general terms, what is required from a nation to implement this recommendation include the following overall capacity and specific capabilities:

- Intellectually: political, legal and technical awareness of cyber threats and incident management and their significance to national and international security;

---

[45] Nicholas Tsagourias, *Risk and the Use of Force* in: Mónika Ambrus, Rosemary Rayfuse and Wouter Werner, (eds.) *Risk and the Regulation of Uncertainty in International Law* (Oxford: Oxford University Press, 2017).

- Organizationally: national cybersecurity structure with differentiated functions and roles and responsibilities for effective incident management, collection and analysis of the information, and decision making;
- Administratively/procedurally: political-level decision making, establishing procedures for information collection, analysis and sharing and for creating sectorial and national situational awareness as well as procedures to evaluate and advance national and sectorial operations;
- Legally: in particular, legislation on network intelligence including monitoring of traffic and events, the mandates of intelligence, analysis and decision-making bodies, information sharing between stakeholders and between the main participants, and legal measures and military responses;
- Technically: capabilities for monitoring, detection, situational awareness, forensic analysis, information sharing and displaying platforms, and defensive and potentially offensive measures;
- Financially: budgetary structure, mechanisms and means to sustain and develop the level and scope of operations.

46. Thus, seen from a postcolonial perspective, the recommendation is unjust. It is also apologetic. It presumes cyberspace to remain a domain of (attributable) State malicious activities and States reprisals, a domain of contestation. A utopian turn away from this insecurity should instead be calling for cooperation, sharing resources and transferring technologies and for refraining from malicious activities, from supporting proxies as well as from adhering to reprisals.

Recommendations

- Having an explicit and published national cybersecurity policy, doctrine or strategy should become a norm of responsible and accountable State behaviour. The notion of national cybersecurity policy, doctrine or strategy,

refers here to all governmental policy and doctrinal documents that seek to provide political guidance by articulating objectives, choosing priorities and allocating resources as well as legitimize the direction and content of taken policy. Such documents, regardless of their name, inform and educate domestic and foreign audiences of government intentions and action within the field of cyber or information security. These documents, as deliberate policy tools, help to create the material, organizational, financial as well as normative foundations of responsible State behaviour. They also establish governmental accountability before people and the international community more effectively than the recommendations of limited groups of experts.

- Facilitate national capacity-building. The recommendation to consider all relevant information assumes such technical, administrative and cognitive capacity to exist in the first place. Governments however are not able to subscribe to the norm without the capacity to monitor national networks, to detect abnormal and malicious activities, to investigate effects and origins of the activities and make justifiable and relevant political decisions. Therefore, internationally facilitated capacity building, not only building networks and ICT systems, but establishing feasible, effective and sustainable national policies, strategies and legislation, is needed; at simplest, including also transfers of technology could help the most vulnerable countries to update or sustain their less-than-optimal operating systems and other software.
- Define concepts, typologies, methods and tools to discuss and handle cyber incidents. Experts and governments, policy-makers and technical personnel, the East and the West, the North and the South do not understand each other. As Ambassador Krutskikh, referring to the 2004-2005 GGE, which he had chaired, explained, "even with the use of translation, the members […] spoke different languages with respect to essential issues related to international information security", notably because of

the lack of "unified and generally accepted definitions of key terms and concepts, and differing interpretations of international law in the area of international information security".[46]

- Moreover, effective use and literally meaningful sharing of information requires a sufficient level of standardization of lexicons, concepts and methods. A groundbreaking advancement would be to agree upon standards of proof in cyber incidents—for example, the parameters of what constitutes sufficient, conclusive, and clear and convincing evidence, as well as principles of burden of proof. This could be done without prejudice and without countries surrendering their sovereign decision-making.
- Investigate international measures that can support the responsible voluntary behaviour recommendation (b) is directly after. Admittedly, global, regional and bilateral measures and capabilities could support countries to better adhere to the norm. Measures that could be deployed rather fast include assessment and reporting tools, at simplest internationally agreed templates, and information sharing platforms. Measures that require proper examination include support to nations to investigate cyber incidents, at simplest bi- or multilateral collaboration, at widest a bilateral, regional or global body with an appropriate mandate and resources.
- On a wider scale, the structure and mechanisms of international cybersecurity should be built on the identified shared areas of concerns. The interlinked clusters include i) the management or policing of undesirable behaviour; ii) maintenance of international relations and global and regional stability; and iii) maintenance and advancement of systemic functionality. These clusters and concerns unite States and the private sector, and States and the individual, and seek to increase predictability and stability of behaviour in and around cyberspace. The question of

[46] United Nations General Assembly, First Committee, A/C.1/60/PV.13 (17 October 2005), p. 7.

attribution mentioned in recommendation (b) and which many commentators went to examine can be solved once the general principles and patterns of behaviour become agreed upon.

Recommendation 13 (c)

States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

Liisi Adamson

Contextualization

1. Recommendation (c) of the United Nations GGE 2015 report reflects the legal concept of due diligence.[1]

2. Due diligence, for some a concept of customary international law,[2] for some a general principle of law[3] and for others merely a standard of behaviour, does not have a uniform definition. It lacks a set standard that would guide all circumstances and all actors equally.[4] Instead, due diligence is a flexible and adaptable concept capable of evolving according

---

[1] Contributions by Kringsak Kittichaisaree, Thomas C. Wingfield, Tang Lan, Prof Nohyoung Park.

[2] Contribution by Kringsak Kittichaisaree.

[3] Karine Bannelier-Christakis, *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?* (Baltic Yearbook of International Law, Vol. 14, 2014), page 4. Timo Koivurova, *Due Diligence* (Max Planck Encyclopedia of Public International Law, 2010).

[4] This was recognised already in 1961 by the Special Rapporteur on the subject of State responsibility Mr. F.V. Garcia Amador, who stated that "The learned authorities are in almost unanimous agreement that the rule of "due diligence" cannot be reduced to a clear and accurate definition which might serve as an objective and automatic standard for deciding, regardless of the circumstances, whether a state was "diligent" in discharging its duty of vigilance and protection." 1957, Vol. II A/CN.4/106, para. 7, page 122 of the commentary to Article 12.

to the changing circumstances.[5] As a result, there have been significant divergences in the application of the principle in scope and in content.[6] Generally, due diligence operates on the standard of reasonableness[7] that is often assessed *ex post facto*, but includes the duty to react and arguably also the duty to prevent. The application of due diligence in the context of state and non-state use of information and communication technologies (ICTs) is topical, especially considering that this concept of international law has historically emerged in order to mediate the relations between states in changing times.[8]

3. Due diligence is tightly coupled with sovereignty[9] and the law of responsibility of states.[10] The broader aim of the principle, however, is to reduce conflicts and provide remedies for those states who have been wronged by other states' actions or omissions.[11] Thus, the goal for the due diligence principle corresponds to the general mandate of the GGE.[12]

---

[5] Seabed Mining Advisory Opinion: "The content of "due diligence" obligations may not easily be described in precise terms. Among the factors that make such a description difficult is the fact that "due diligence" is a variable concepts. It may change over time." 2011, 50 ILM 458, para. 117. See also, Duncan French (Chair) and Tim Stephens (Rapporteur), *ILA Study Group on Due Diligence in International Law. First Report* (7 March 2014), page 2.

[6] Especially taking into account that due diligence has been particularised in the specialised regimes of international law, such as international environmental law, international humanitarian law and human rights law. Duncan French and Tim Stephens, op. cit., page 3.

[7] Contribution by Thomas C. Wingfield states that the standards of reasonableness is a fairly low one, which floats with the level of state's ICT capability.

[8] ILA Study Group on Due Diligence in International Law. First Report, page 2.

[9] Most fundamentally, due diligence flows from the concept of sovereignty; however, it can in specific circumstances also derive from the principle of good neighbourliness. See Joanna Kulesza, *Due Dilience in International Law* (Leiden-Boston: Brill, Nijhoff 2016), page 260.

[10] For an elaborate discussion the relationship between due diligence principle and state responsibility, see Timo Koivurova, op. cit.

[11] Joanna Kulesza, op.cit, page 1.

[12] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174), para. 1-2.

4. This particular construction of the principle in recommendation (c), differing from the general maxim known from international jurisprudence,[13] needs to be placed in the wider context of state actors, non-state actors, harm and standards of due diligence (such as knowledge, feasibility, reaction, prevention, risk). Due to the inter-connected nature of the information infrastructure and architecture, the occurrence of transboundary harm is likely. Thus, the most practical aim of said principle is to minimise harm that could have a transboundary effect.

5. While some of the recommendations in the GGE 2015 report respond to more specific threats, recommendation (c) establishes a baseline for state accountability in instances where transboundary harm emanates from its territory, but there is no clear attribution of activities and application of state responsibility towards the state. To that extent, the recommendation addresses a variety of threats outlined in the reports pertaining, inter alia, to the critical infrastructure, terrorist use of ICTs, non-state actors (as proxies and as perpetrators), and capacity differences.[14] The GGE has repeatedly acknowledged that threats can emanate from state as well as non-state actors.[15] Due diligence is one of the principles that generally addresses both sources of threats.

6. Recommendation (c) relates to several other parts of the 2015 report. As one strand of interpretation of the due diligence principle includes also preventive actions, the recommendation has direct connection to cooperation and confidence-building

---

[13] In particular see ICJ, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), 1949, ICJ Rep 4, p. 22: "A State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."

[14] Full list of threats are outlined in *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 30 July 2010 (A/65/201), Chapter II. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98), Introduction. A/70/174, Chapter II.

[15] Ibid.

measures (CBMs).[16] Another aspect of the due diligence principle is also feasibility of actions taken to stop the harmful activity, which is directly linked to the capacity of the states. Capacity building is also one of the ways to fortify and exercise due diligence, especially considering states who might be described as "unable" states, who are not able to comply with the due diligence principle. The measures that can be considered *feasible* in their specific context are not up to par with the capacities of other countries. Therefore, recommendation (c) has a close link also to the capacity building section of the report,[17] because enhancing the capacity of states to stop and prevent certain malicious activities enhances the stability, predictability and security of the whole international community.

7. The most apparent connection exists between recommendation (c) and the international law section. Namely, the recommendation at hand represents the general due diligence obligation, while being located in the voluntary non-binding norms section. Due diligence as a principle flowing from the concept of sovereignty is inherently an international law principle. The international law section sets forth first that "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."[18] The general due diligence principle applies to state as well as non-state actors, as due diligence applies throughout the sovereign territory of a territorial state. This means that, according to Schmitt, the due diligence principle is encompassing any infrastructure, architecture, activities or people who are carrying out cyber operations in the said territory.[19] Secondly, recommendation (c) does not textually distinguish between different actors. Interestingly, the international law section, however, puts

[16] A/70/174, Chapter IV.
[17] A/70/174, Chapter V.
[18] A/70/174, para. 27. Also stated in the A/68/98, para. 20.
[19] Michael N. Schmitt. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Second Edition (Cambridge University Press, 2017), page 32.

forth a separate paragraph on specifically non-state actors and their activities vis-à-vis the territory of a state. The paragraph states, "[States] should seek to ensure that their territory is not used by non-state actors to commit such acts [refers back to internationally wrongful acts]." Interpreting the due diligence principle vis-à-vis states and their obligation for non-state actors, the recommendation and the international law section are closely connected. Recommendation (c) also links to the international law section by the fact that it applies the notion of "internationally wrongful act", which is a term of art referring to state responsibility under international law.

Background

8. Due diligence represents a long-standing desirability that states as members of international community adhere to certain behavioural standards or seek to achieve certain outcomes.[20] In an age, where inter-connected technologies, networks and the use thereof can have transboundary effects, controlling harm that might emanate from states' territory is of utmost importance. Consequently, when applied, the concept of due diligence would ensure predictability of behaviour.

9. The utility of the concept is supported in several states' contributions that have taken part of the GGE process. In 2003, the Russian Federation presented a proposal for a security arrangement that would provide that, "States and other subjects of international law must bear international liability for activities in information space which they carry out or which are carried out from territory under their jurisdiction."[21] In 2011, Germany acknowledged the need to start a debate on "State responsibility for cyberattacks launched from their territory when States do nothing to end such attacks despite being informed about

[20] Duncan French and Tim Stephens, op. cit., page 46.

[21] *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, Submission by Russian Federation, A/58/373, page 11.

them."[22] Similarly, the Netherlands has put forward in 2015 that, "Of particular importance is the examination of the international legal framework that applies to cyber operations that do not rise to the threshold of an armed attack. […] [This] includes the question of the application of the principle of due diligence, i.e. not knowingly allow a State's territory to be used for acts contrary to the rights of other states."[23]

10. Even though there is no treaty that would uniformly set the standards of due diligence, it is a very developed principle in several particular contexts of international law. Following the developments of specialised fields, a large amount of jurisprudence (judicial and arbitral) has been developed that addresses the content and boundaries of the due diligence principle. In 1872, the Alabama Claims arbitration between United States and Great Britain that recognised that due diligence was "a failure to use for the prevention of an act which the government was bound to endeavor to prevent, such care as governments ordinarily employ in their domestic concerns, and may reasonably be expected to exert in matters of international interest and obligation."[24] Recognizing thereby not only the existence of the due diligence obligation but also the fact that prevention aspect is corollary to the due diligence obligation.[25] The Trail Smelter arbitration that declared that, "no State has the right to use or permit the use of its territory in such a manner as to cause injury […] in or to the territory of another or the properties or persons therein, when the case is of

---

[22] *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, Submission by Germany, A/66/152, page 10.

[23] *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, Submission by Kingdom of the Netherlands, A/70/172, page 4.

[24] Case presented on the part of the government of her Britannic Majesty to the Tribunal, in Papers Relating to the Foreign Relations of the United States 412, 1872.

[25] Alabama Claims of the United States of America against Great Britain, Award rendered on 14.09.1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 08.05.1871, United Nations, Reports of International Arbitral Awards, Vol. XXIX, page 130.

serious consequence and the injury is established by clear and convincing evidence".[26]

11. The Permanent Court of International Justice (PCIJ) and the International Court of Justice (ICJ) have followed suit. In the SS Lotus Case in 1927, PCIJ stated that, "[i]t is well settled that a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people."[27] The most famous maxim of state's due diligence obligation, and also the dictum on which recommendation (c) is based on, derives from the Corfu Channel case, which put forth that it is "[e]very State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[28]

12. However, it must be noted that there has been some hesitance about accepting and applying the principle of due diligence in general as well as to various ICT activities.[29] This uncertainty goes back to the work of the International Law Commission (ILC) on the State Responsibility Project, where the principle of due diligence was excluded from the original remit of the project as a controversial issue.[30] The hesitance has continued, some argue, because of the extent of obligations that such a principle would impose on states.[31] Both transit states and "highly" connected states might face, especially in the context of interconnected ICTs and networks, a disproportionate burden when accepting the applicability of the said principle. A merely legal argument might be that there is insufficient state

---

[26] Trail Smelter Case (US vs. Canada), 3 Rep. Int'l Arbitral Awards 1905, 1965 (11 March 1941).

[27] SS Lotus (France vs. Turkey) 1927 PCIJ (Ser.A) No 10.

[28] ICJ, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), 1949, ICJ Rep 4, p. 22.

[29] Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace* (Yale Law Journal Forum, 2015) pages 71-73.

[30] Similarily, in the context of negotiations of the Watercourses Convention, Koivurova points out that "it became apparent that references to the concept of due diligence would have to be removed in order for the Watercourses Convention to be concluded." Timo Koivurova, op. cit.

[31] Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, Yale Law Journal Forum, 2015, page 71-73. Contribution by Tang Lan.

practice and *opinio juris* to extend the due diligence principle to contexts other than the specialised fields already recognised by states.[32]

13. Despite other informed approaches, it is evident to this author that due diligence is a well-settled concept of international law. Consequently, situating recommendation (c), which in content is textually identical to the general dictum of due diligence with the addition of "using ICTs" and exchanging "contrary to the rights of other States" with "internationally wrongful acts" in the voluntary norms, rules and principles section, constitutes a political move. Alternatively, recommendation (c) could be read as selectively and partially invoking some of the standards deriving from the legal concept of due diligence and outlining it in the voluntary norms part as an ICT-specific standard that does not readily flow from established international law.

14. The rest of the commentary is written from the standpoint whereby a general duty of due diligence exists under international law. The principle of due diligence,[33] deriving from the concept of sovereignty,[34] has been reaffirmed multiple times in the international jurisprudence.[35] The dictum put forth in the *Corfu Channel*[36] has been accepted as a general principle of international law.[37] Therefore, recommendation (c) in its current

---

[32] Ibid.

[33] For a historical overview of the due diligence principle, see Joanna Kulesza, op. cit., Chapter 1.

[34] A corollary of sovereignty is the duty "to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and in war ...." Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928).

[35] Island of Palmas Case (Netherlands vs. USA), 4 April 1928, Reports of International Arbitral Awards, United Nations, Vol II, p 839. ICJ, ICJ, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), 1949, ICJ Rep 4, p 22. PCIJ, SS Lotus Case (France v. Turkey), 1927, Ser. A, No. 10, at 88. Trail Smelter Case (US vs. Canada), 3 Rep. Int'l Arbitral Awards 1905, 1965 (11 March 1941). Nicaragua case, para. 157. Tehran Hostages case, paras 67-68.

[36] Corfu Channel, op. cit., page 22

[37] According to Bannelier-Christakis this understanding forms the basis of the contemporary understanding of due diligence. Karine Bannelier-

wording is nearly identical with the dictum recognised at least as a general principle of law. In this sense, it is not a proposal for a future norm or "merely" an idea or a vision.[38] Moreover, a close textual reading of the recommendation highlights several constraints that it establishes on the due diligence obligation. Thus, it can be argued that recommendation (c) raises some of the standards deriving from the general dictum and this specific ICT-related standard might indeed belong to the norms section.

Expansion and analysis

15. Bannelier-Christakis argues that duty of care vis-à-vis ICT-related activity goes beyond the territory of state. It covers all activities, which take place under the jurisdiction or control of states.[39] As a general principle of law, the due diligence obligations and similarly recommendation (c) apply to cyber activities, regardless if they are considered high or low intensity and whether the harmful ICT-related activity is launched from the territory of a state or just routed through a state.[40]

16. The general principle of due diligence addresses two kinds of actors: states and non-state actors. When identifying the said actors, there is also a need to distinguish the target state of the harmful activity, the territorial state that is the subject of the due diligence obligation (transit state or state that needs to counter-act the activities of non-state actors on its territory) and the third party, that is the author of the harmful activity (state or non-state actor).[41] As elaborated before, recommendation (c) does not differentiate between the perpetrators. From the logic

---

Christakis, op. cit., page 4. Michael N. Schmitt, Tallinn Manual 2.0, page 30.

[38] Contribution by Myriam Dunn Cavelty, page 1.

[39] Karine Bannelier-Christakis, op. cit., page 4. Michael N. Schmitt, Tallinn Manual 2.0, page 32.

[40] Michael N. Schmitt, Tallinn Manual 2.0, page 32; K. Bannelier-Christakis, op. cit., page 6.

[41] Michael N. Schmitt, Tallinn Manual 2.0, page 32.

of the general due diligence principle, it should be considered to apply to both state and non-state actors.[42]

17. At the same time, recommendation (c) limits the application of due diligence to acts that can be qualified as "internationally wrongful acts".[43] This specification, on the one hand, seems to impose a stricter standard to the due diligence obligation. The wording of internationally wrongful acts, a term of art in the discourse of the international responsibility of states, delimits the recommendation to exclude accidents (i.e. limits it to only intentional activities), but also could be construed as excluding cases of liability, thus also non-state actors. Generally, it is agreed that states, rather than individuals or private entities violate international law and commit internationally wrongful acts.[44] The general dictum refers to the violation of "rights" of other states, lending itself to a wider interpretation. Such violations can be understood to comprise all unlawful acts that produce detrimental effects on another state.[45] Internationally wrongful act, on the other hand, as defined by the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, exists if there is an action or omission that is attributable to a state under international law and such act constitutes a breach of an international obligation of the state. A breach of an international obligation exists "when an act of that state is not in conformity with what

---

[42] Michael N. Schmitt, Tallinn Manual 2.0, page 32.

[43] This is different from the dictum set out in the Corfu Channel case, which stated that the acts that need to be mitigated are acts "contrary to the rights of other States". Tallinn Manual equates the dictum with internationally wrongful acts. Michael N. Schmitt, Tallinn Manual 2.0, page 34.

[44] Michael N. Schmitt, Tallinn Manual 2.0, page 36.

[45] Karine Bannelier-Christakis, op. cit., page 4. J.G. Lammers, "States are not only obliged to prevent violations of those rights committed by their organs but are also obliged to prevent inroads on the interests protected by those rights by the conduct of individuals or private entities from within their territories." J.G. Lammers, *Pollution of International Watercourses* (The Hague: Nijhoff 1984), page 527, cited in ILC, Second Report on the Law of the Non-Navigational Uses of International Watercourses, by Stephen C. McCaffrey, Special Rapporteur, Yearbook of the International Law Commission, 1986, page 116, footnote 191.

is required of it by that obligation".[46] By this interpretation, recommendation (c) would exclude the activity of non-state actors that is not attributable to the state and mitigation of which would fall under the due diligence obligation. This narrow textual reading would thus mean that recommendation (c) applies only to transit states and covers only acts by states as well as non-state actor activity that is attributable to state. Recommendation (c) thereby leaves out the due diligence principle aspect that states are also responsible for mitigating transboundary harm emanating from their territory created by non-state actors on their territory (but which is not attributable to them).[47] This brings the line of questions back to the fact that such activity, apparently excluded in recommendation (c) in the non-binding norms, rules and principles section, is in the United Nations GGE 2015 report addressed under the international law section, which states consider binding. It leaves unanswered the question whether such omission is intentional or accidental, and thus, the possibility prevails that the GGE has indeed wanted to restrict the concept in the context of state uses of ICTs.

18. According to the Tallinn Manual approach, categorisation of the acts as internationally wrongful acts for the purposes of the due diligence principle posits no problems: non-state actors' activity will be assessed on the basis of comparing their activities with those of states. If other prerequisites are fulfilled (i.e. the harmful activity results in serious adverse consequences and affects the target state), then the due diligence obligation can be invoked, if the activity, if conducted by a territorial state, would constitute an internationally wrongful act.[48] For example, if a cyber operation conducted by a non-state actor would amount, if conducted by a state, to a breach of sovereignty, which is an internationally wrongful act, the state would have

---

[46] ILC. Draft Articles on the Responsibility of States for Internationally Wrongful Acts, 2001. Article 2, Article 12.

[47] One of the commentators Anatoly A. Streltsov agreed with the approach, stating that the recommendation (c) focuses only on states and does not focus on non-state actors, encompassing only "State territory used by other States for commission of internationally wrongful acts". Commentary by A. Streltsov.

[48] Michael N. Schmitt, Tallinn Manual 2.0, pages 35-36.

a due diligence obligation in this instance. At the same time, the question remains, if non-state actor activity does not violate international law per se[49] then to what extent can we apply this analogy comparing states with non-state actors in instances where there is no primary norm applicable to non-state actors that such activity would breach. Following the Tallinn Manual conclusion, due diligence as a binding international law principle applies to non-state actors via analogous interpretation even if there is no primary international law obligation. From the wording of the international law section, the GGE could be argued to agree that due diligence obligation vis-à-vis non-state actors is a binding obligation, but recommendation (c) concludes to the contrary that due diligence obligation vis-à-vis state activities transited through a second state, do not give rise to a binding due diligence obligation for the transit state.

19. The core of recommendation (c) and more generally of the due diligence principle is to provide a standard of care against which state conduct can be assessed. It is to a large extent a standard of reasonableness. Such reasonable care standard seeks to take into account the *consequences* of the wrongful conduct and the extent to which such consequences could *feasibly* have been avoided by the state if it had *knowledge* of the wrongful conduct.[50] As a standard of reasonableness, the general principle of due diligence does not prescribe the precise result or timeframe by which the state has to achieve the said outcomes.[51] Thus, recommendation (c) as a due diligence principle is an obligation of knowledge, reaction and arguably also of prevention.[52] It is a standard of reasonableness necessitating action from states where mitigating an instance is feasible.

---

[49] Non-State actors' activity is generally addressed under domestic laws of each State.

[50] ILA Study Group on Due Diligence in International Law, Second Report, page 2.

[51] ILA Study Group on Due Diligence in International Law, Second Report, page 46. Scott J. Shackelford, Scott Russell, Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors* (17 Chi. J. Int'l L. 2016), page 34.

[52] Karine Bannelier-Christakis, op. cit., page 15.

20. Tallinn Manual 2.0 establishes two rules pertaining to the due diligence principle. Firstly, it states that, "[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[53] To that end, "[t]he principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States."[54]

21. Carving out the margins of the due diligence principle in the context is no easy task.[55] Due to the flexible and relative nature of the said obligation, specific criteria depend on the circumstances of the case and, thus, limit the description to the more general traits of due diligence.[56] A series of United States and Mexico arbitrations have put forth that, "while the content of due diligence cannot be precisely defined, a series of objective factors may be taken into account in determining the content of the due diligence obligation in any particular case."[57] Factors proposed by the said arbitrations modified for the context of ICTs that could be taken into account for the commentary at hand include:

- Degree of effectiveness of the state's control over [infrastructure and architecture on its] territory [and under

---

[53] Michael N. Schmitt, Tallinn Manual 2.0, page 30.

[54] Michael N. Schmitt, Tallinn Manual 2.0, page 43.

[55] Contribution by Tang Lan.

[56] Joanna Kulesza, op. cit., page 264.

[57] ILA Study Group on Due Diligence in International Law, First Report, page 3. Riccardo Pisillo-Mazzeschi has identified four key challenges to the application of the due diligence principle. It must be determined what level of due diligence is required of states in their activities, and whether that standard should be determined universally or rather in reference to individual state practice. Secondly, is the obligation of due diligence a subjective or objective obligation. Thirdly, whether the content of the commitment the principle endows is fixed or flexible. And lastly, what are the limits of due diligence. Riccardo Pisillo-Mazzeschi, *The "Due Diligence" Rule and the Nature of the International Responsibility of States* (1992, 35 GYIL 9-49), page 40. See also, Joanna Kulesza, op. cit., page 263.

its jurisdiction] with the State being required to take all necessary steps to ensure its effectiveness;[58]

- Degree of predictability of harm, including "predictability of damage, having considered all possible and reasonable state efforts aimed at obtaining necessary knowledge on the risks and threats";[59]
- The importance and weighing of the interest to be protected by the state.[60]

22. As the determination of whether a state has abided by its due diligence obligation is always an *ex post facto* analysis, similar criteria could be taken into account while substantiating the due diligence obligation in the context of ICTs. Moreover, due diligence is an objective standard, application of which might necessitate reference to certain subjective conditions as well, seeing that due diligence is largely also a question of capacity and action.[61]

23. Certain degree of *harm* is a prerequisite of invoking the obligation deriving from recommendation (c). The extent of harm is in correlation with the activities that states have to take to fulfil the due diligence obligation. The conduct that is expected of states in the cases of transboundary harm is in "exact proportion to the risks".[62] Thus, the scope of the due diligence obligation may change in relation to the risks involved in the activity.[63]

---

[58] For example if the infrastructure belongs to the private sector, it is up to the state to make sure that there are effective public-private partnerships in place that would allow rapid mediation of incidents, if necessary.

[59] Joanna Kulesza, op. cit., page 264.

[60] ILA Study Group on Due Diligence in International Law, First Report, page 3. Joanna Kulesza, Due Diligence in International Law, page 264.

[61] See the discussion of feasibility of taking mitigating measures. Joanna Kulesza, op. cit., page 263-264.

[62] ILA Study Group on Due Diligence in International Law, First Report, page 31. Alabama Claims Arbitration.

[63] Seabed Mining Advisory Opinion, 2011, 50 ILM 458, para. 117. Also reflected in the ILC's Draft Articles on the Prevention of Transboundary Harm. Commentary of Article 3 explains that due diligence standard should be appropriate and proportional to the degree of risk of the transboundary harm. ILC, Draft Articles on Prevention of Transboundary

24. Even though predictability of harm is considered one of the aspects of the due diligence obligation, the said obligation is not an absolute one. The principle *sic utere tuo ut alienum non laedas* assumes that the target or victim states must accept some level of harm.[64] States cannot be expected to predict and prevent every harm. Hereby, the standard is still one of reasonableness. There are two standards attached to the question of harm. Firstly, what is the level of harm needed for invoking the due diligence obligation. And secondly, to what extent must harm be known to the state under the due diligence obligation; i.e. what does the standard of "knowingly" entail in recommendation (c) and does the due diligence obligation also entail preventive activities.

25. The Tallinn Manual 2.0 puts forth that a standard from environmental law could be helpful for contextualising harm. Namely, a cyber operation ought to result in *serious adverse consequences* in order to invoke the due diligence obligation.[65] There is no single primary norm in international law that would set out the standard of harm for ICT-related activities. International Telecommunication Union establishes standards for the "no harm" principle and a norm for "harmful interference";[66] however, even in those instances of technical harm, the exact scope of these thresholds, i.e. what constitutes harm, is not clear.[67] However, in the context of due diligence obligation, it is claimed that the objective standard of the said obligation is independent of the nature of the harm,

---

Harm from Hazardous Activities, United Nations GAOR 56th Session, Supp. No. 10, United Nations Doc. A/HRC/17/31 (March 21, 2011), Commentary to Article 3, para. 11.

64 The view that the victim state must accept some harm derives from the doctrine of good neighbourliness. Timo Koivurova, op. cit., page 236. Eric Talbot Jensen, Sean Watts, *A Cyber duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?*, page 1566.

65 Michael N. Schmitt, Tallinn Manual 2.0, page 37.

66 ITU Constitution, Article 42, Article 45. ITU ITRs, Article 9.

67 A contribution to this commentary by Richard Hill proposed that recommendation (c) could be subsumed under the Article 6 of ITR's. However, the interpretation of limiting harm in the due diligence context to solely technical harm is too narrow.

representing thus merely a primary standard of conduct.[68] This is corroborated by the Tallinn Manual approach, which claims that one ought to not assess the nature of harm, but look at the extent of consequences (serious and adverse).[69] What the thresholds are for such assessments and what kind of harm we can categorise as serious and adverse have not been identified.[70]

26. The second prerequisite put forth by recommendation (c) is *knowledge*. In order to invoke the due diligence obligation, the state needs to have had knowledge of the said harmful activity.[71] Nevertheless, states cannot have *absolute* knowledge of all activities that are happening on its territory.[72] The situation is complicated by the fact that in several cases (e.g., for transit states) it would be impossible to prove that there was knowledge of harmful ICT-related activities. Even if such knowledge exists, the available time for an adequate reaction is also of importance.[73] Taking into account the rapidness of the ICT activities, it could create a situation where a transit state

---

[68] Joanna Kulesza, op. cit., page 31.

[69] Michael N. Schmitt, Tallinn Manual 2.0, page 37.

[70] The question also remains, what substantive differences are between "serious" and "substantive", "significant". Jolley bases the question of the level of harm off of the Trail Smelter arbitration and the rule accepted in customary international law by claiming that harm must be significant or substantial. Jason D. Jolley, *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law* (PhD Thesis, University of Glasgow, 2017), page 188-190.

[71] ICJ in the Tehran Hostages case, "Iranian authorities were fully aware of the urgent need for action on their part, had the means at their disposal to perform their obligations and completely failed to comply with these obligations." ICJ, United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), 24.05.1980, ICJ Reports 1980, para. 68.

[72] ICJ put forth in the Corfu Channel case that it cannot be concluded from the mere fact of the control exercised by a state over its territory and waters that that state necessarily knew or ought to have known what was happening on its territory. Corfu Channel case, page 18.

[73] Karine Bannelier-Christakis, op. cit., page 6. ICJ has also stated in the Corfu Channel case that the availability of enough time in order to notify third states and to react is very important in order to assess if a state failed in relation to its due diligence obligation. Corfu Channel case, page 22.

would not be held accountable for violating the due diligence principle.[74]

27. Due diligence can be said to apply in instances where a state has *actual knowledge* about the harmful activity against other states. For example, according to Schmitt, this is the case, where state organs have received credible information to the fact or the intelligence services have detected hostile activity themselves.[75] However, interpreting recommendation (c) and the due diligence principle in the wider sense as establishing responsibility for activities only in cases of actual knowledge narrows the standard overly much. Therefore, it is also accepted that there are instances where states ought to have known about a specific harmful situation. *Constructive knowledge* standard applies if a state, using reasonable care and diligence, should have become aware of the harmful use of its territory.[76] In this case, due diligence is breached, "if the state is in fact unaware of the cyber operations in question, but objectively should have known that its territory was being used for the operation."[77] Constructive knowledge can be deduced for example from the probability of malicious cyber attacks originating from the territory, the past history and repeated or continuous malicious harmful cyber operations originating from the state's territory, or direct use of state-controlled critical infrastructure.[78] Thus, the due diligence obligation arises for the state upon obtaining knowledge (actual or constructed) of an unauthorised, risky activity carried out within state territory, under its jurisdiction or control.

---

[74] Karine Bannelier-Christakis, op. cit., page 6.

[75] Michael N. Schmitt, Tallinn Manual 2.0, page 40.

[76] Michael N. Schmitt, Tallinn Manual 2.0, page 41.

[77] Michael N. Schmitt, Tallinn Manual 2.0, page 41.

[78] Scott J. Shackelford, Scott Russell, Andreas Kuehn, op. cit., page 20-21. Shackelford et al. also note that "knowledge must be understood in context, as the individual packets transmitted through the State's network may, if taken alone, be innocuous." Shackelford et al, page 21. Jolley notes similarly a word of caution, stating that, "The more advanced the cyber infrastructure of a State, or the more control the State exerts over its infrastructure, the higher the likelihood of imputed knowledge of cyber attacks." Jason D. Jolley, op. cit., page 196.

28. Thus, the standard of knowledge in due diligence is a rather high one. Moreover, paragraph 28 (f) in the international law section sets forth that "accusations of organising and implementing wrongful acts brought against states should be substantiated".[79] Applying the same logic, it can be implied that claims of breaches of international obligations, i.e. the due diligence principle, should be substantiated as well. Evidence and standard of proof in ICT and due diligence–related cases may be hard to provide, especially if the evidence is not within their territory or jurisdiction. In such instances, the international community has applied the standard "no room for reasonable doubt"[80] if circumstantial evidence is used. Hence, the mere fact that the activity occurred in the state's territory is not evidence of knowledge; however, cases where, for example, the state's non-commercial critical infrastructure that the state has full control over is used may serve as an argument to presume that the state had or should have had knowledge of the harmful activity.[81]

29. Admitting that there are instances where states should be aware of what is happening on their territory and jurisdiction, leads to the question of whether recommendation (c) invites states to monitor activities on their territory and in their

[79] A/70/174, para. 28(f).

[80] This derives from the Corfu Channel case. ICJ stated, "the fact of this exclusive territorial control exercised by a State within its frontiers has a bearing upon the methods of proof available to establish the knowledge of that State as to such events. By reason of this exclusive control, the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility." For this reason, victims should, "be allowed a more liberal recourse to interferences of fact and circumstantial evidence. […] The proof may be drawn from inferences of fact, provided that they leave no room for reasonable doubt." The burden of proof might also be not only on the victim accusing another State of a breach of its obligations, but the State on whose territory the act occurred, "may be called upon to give an explanation (and) cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and of its authors." Corfu Channel case, page 18, page 42.

[81] Scott J. Shackelford, et al., op. cit., page 10.

jurisdiction.[82] Proponents of monitoring activity connect the duty to monitor with the fact that due diligence can also be interpreted as a preventive norm.[83] However, it must be noted that, most likely, recommendation (c) or the general due diligence obligations do not foresee constant monitoring activities.[84] Due diligence activities have to be compatible with international law as well.[85] The requirement of knowledge cannot legitimise violations of, for example, human rights or privacy rules.[86] Therefore, recommendation (c) could be interpreted as inviting continuous reasonable efforts in good faith in order to obtain information about potentially hazardous activities. Thus, the obligation to monitor the risky activity ought to arise when the state obtains knowledge of the said activity.[87]

30. Whether the due diligence obligation entails only the duty to mitigate threats that pertain to known harm, or whether it encompasses preventive activities towards certain predictable

---

[82] ICJ has stated in the Pulp Mills case that due diligence implied, "the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party." Pulp Mills, para. 197.

[83] For example, Karine Bannelier-Christakis, op. cit., page 8. She also submits that for example French White Book on Defence "presents monitoring as a cornerstone in the fight against cyber activities, which are dangerous for the security of States." Ibid., page 8. See also Thomas C. Wingfield's contribution: "Doctrine of due diligence requires States to take reasonable measures to surveil and control bad actors on their ICT networks."

[84] Michael N. Schmitt, Tallinn Manual 2.0, page 40-43.

[85] ICJ in the Genocide case: "it is clear that every State may only act within the limits permitted by international law." Genocide case, para. 116. Karine Bannelier-Christakis, op. cit., page 8.

[86] The Right to Privacy in the Digital Age resolution by United Nations GA in 2013 offers guidance on what states should respect in this domain. A/RES/68/167 the Right to Privacy in the Digital Age, 18.12.2013.

[87] Joanna Kulesza, op. cit., page 192. Cf. ICJ, Genocide judgment, "a state's obligation to prevent, and the corresponding duty to act, arise at the instant that the state learns of the existence of a serious risk that the act will be committed." Genocide judgment, para. 431.

harm as well, is a disputed question.[88] Most experts in the Tallinn Manual team took the position that the due diligence obligation is not a preventive one.[89] ILC has taken a similar position in the Draft Articles when it stated that "[t]he breach of an international obligation requiring a state to prevent a given event occurs, when the event occurs."[90] In the clearest cases, due diligence obligation applies when harm occurs and can be invoked from the moment harmful consequences manifest.[91] On the other hand, the United States–Mexico Claims Commissions have stated in the Youmans case that a state must satisfy its duty of prevention in order to fulfil its due diligence obligation, something that Mexico failed to do and, thus, also failed to abide by its due diligence obligation by not preventing the attack resulting in the death of American citizens.[92] The Corfu Channel case that elaborated the modern dictum of due diligence also states that "[n]othing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania."[93] In the context of

---

[88] Karine Bannelier-Christakis finds for example that there is a dual obligation of acting and preventing. K. Bannelier-Christakis, op. cit., page 6.

[89] Michael N. Schmitt, Tallinn Manual 2.0, page 42, 45.

[90] Draft Articles on the State Responsibility, Article 14(3). In full: "The breach of an international obligation requiring a State to prevent a given event occurs when the event occurs and extends over the entire period during which the event continues and remains not in conformity with that obligation."

[91] Karine Bannelier-Christakis, op. cit., page 13. R. Ago "To our knowledge, decisions of international tribunals have never affirmed, even indirectly or incidentally, that failure to adopt measures to prevent the occurrence of a possible event sufficed in itself- i.e. without the actual occurrence of such an event—to constitute a breach of the obligation incumbent on the State. R. Ago. Seventh report in State Responsibility, ILC Yearbook 1978, para. 11, page 34.

[92] Thomas H. Youmans (USA) v. United Mexican State, 23.11.1926, United Nations, Reports of International Arbitral Awards, Vol 4, para. 12, page 115.

[93] Corfu Channel case, page 23. Note also that the Alabama Claims tribunal noted also that prevention obligation is corollary to the due diligence obligation. "The British government failed to use due diligence in the performance of its neutral obligations; and especially that it omitted, notwithstanding the warnings and official representations made by the

recommendation (c) and the broader ICT application of the said recommendation, the question arises whether it entails also the obligation of prevention or is it merely a reactive recommendation.

31. It is clear that a general obligation of prevention of unknown future transboundary harm is disproportionate towards states. On the one hand, taking into account the speed of operations in cyberspace, preventive measures that are proportionate to the risk of potential harm might be more effective than mitigation of ongoing incidents.[94] On the other hand, duty to react and duty to prevent should not create an impossible burden for states.[95] The diligence that is due cannot exceed a state's capabilities.[96] However, to the extent that the harm is foreseeable, if a state has knowledge that such harm might occur and if feasible measures to stop this harm exist, the due diligence obligation might apply. An example would be when a state can foresee with reasonable certainty that cyber infrastructure on its territory that has been used for harmful activity before will be employed again for such activities against another state and it has the capacity to take appropriate measures

---

diplomatic agents of the United States during the construction of the said number '290', to take in due time any effective measures of prevention, and that those orders which it did give at last, for the detention of the vessel, were issued so late that their execution as not practicable." Alabama Claims Tribunal, page 130. Similarly, in the context of international humanitarian law, ICJ held, in the case pertaining to the Armed Activities on the Territory of the Congo, the Congo responsible, "for any lack of vigilance in preventing violations of Human Rights and International Humanitarian Law by other actors present in the occupied territory, including rebel groups acting on their own account." ICJ Armed Activities on the Territory of The Congo (Democratic Republic of the Congo vs. Uganda), 19.12.2005, ICJ Reports 2005, para. 179.

94 Michael N. Schmitt, Tallinn Manual 2.0, page 45-46. This is an approach that no-one in the Tallinn Manual team agreed with.

95 Karine Bannelier-Christakis gives an overview of human rights bodies, which have largely agreed on the same matter and cautioned again for the application of the criteria of reasonableness. Karine Bannelier-Christakis, op. cit., Page 10. Michael N. Schmitt, Tallinn Manual 2.0, page 44.

96 Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, Yale Law Journal Forum, 2015.

to secure the infrastructure as to thwart future attacks.[97] This obligation, to foresee certain activities, is higher in instances where manifestation of such harm is based off of very public information (e.g., Heartbleed case, Wannacry). Thus, due diligence applies also in cases of specific cyber activity that have not yet been launched, but material steps towards execution of such operations are being taken and a reasonable state would conclude that the operation will be carried out.[98] Moreover, prevention standards in the due diligence context ought to be evaluated with regard to the current developments in the ICT activity.[99]

32. Assuming that a state has knowledge of the harmful ICT-related activity, recommendation (c) does not elaborate on what measures states should take. Generally, the due diligence principle obliges states to take all *feasible* measures to mitigate or terminate any harmful activity emanating from its territory, as due diligence is an obligation of conduct, not one of result.[100] Such obligation generally entails a state's best efforts or doing all that is feasible in particular circumstances to achieve the desired outcome.[101] It has been put forward that the term "best

---

[97] Michael N. Schmitt, Tallinn Manual 2.0, page 47-48. Additionally, a question arises pertaining to the capabilities of developing states. Such interpretation could put developing countries in a significant disadvantage, because the due diligence obligation applicable to them, if they have infrastructure that is constantly used for such harmful activity, would be much higher than the general standard. This is mitigated by the fact that due diligence takes into account the capabilities of states, but the balance between the obligation (objective) and considering capabilities (subjective) is debatable.

[98] Michael N. Schmitt, Tallinn Manual 2.0, page 43.

[99] Joanna Kulesza, op. cit., page 194.

[100] Michael N. Schmitt, Tallinn Manual 2.0, page 43-50; ILC, Draft Articles on the Law of the Non-Navigational Uses of International Watercourse and Commentaries thereto and Resolution on Transboundary Confined Groundwater, Report of the International Law Commission on the Work of its Forty-sixth Session, 1994. Commentary of Article 7. As to the case law, see Pulp Mills, paras 186-187.

[101] ILC: "Obligations of prevention are usually construed as best efforts obligations, requiring states to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur." ILC Draft Articles on Responsibility of States

efforts" could create a grey area between normative and merely political obligations, thus, it might be better to frame states' obligations as one to "employ all available means" or "to take all available measures" or "to do all that could be reasonably expected of them."[102] Feasibility implies that the deciding factors for the content and extent of activities, that the state must take in the framework of its due diligence obligation, are the state's actual capabilities for counteracting harmful cyber acitivity.[103] Hence, feasibility of certain measures is always contextual[104] and depends, inter alia, "on the technical wherewithal of the state concerned, the intellectual and financial resources at its disposal, the state's institutional capacity to take measures, and the extent of its control over cyber infrastructure located on its territory."[105] Therefore, as an obligation of conduct, not one of result, the analysis of acts contrary to recommendation (c) need to take into account the level of effort the state showed in order to meet the due diligence obligation. It is a balancing act between harm, knowledge of said harm, capabilities of the state and the effort taken to mitigate the transboundary harm.[106]

---

for Internationally Wrongful Acts with commentaries, Report of the International Law Commission on the work of its fifty-third session, 2001, page 62.

[102] K. Bannelier-Christakis, op. cit., page 5. See also ICJ, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), 26.02.2007, ICJ Reports 2007, para. 430.

[103] Quentin-Baxter and Barboza conceived the standard of due diligence in the context of prevention to be proportional to the degree of risk of transboundary harm in a particular case. The standards should take into account the means at the disposal of the state and the standards applied in the affected state, in regional and international practice. First report on prevention of transboundary damage from hazardous activities, Yearbook…1998, vol II (Part one), document A/CN.4/487 and Add. 1, page 191, para. 55(f).

[104] Contribution by A. Streltsov also states that one should consider objective and subjective facts.

[105] Michael N. Schmitt, Tallinn Manual 2.0, page 47. Genocide judgment, paras 430-431. Tehran Hostages judgment, paras 63-68. Armed Activities judgment, para. 301.

[106] ILA Study Group on Due Diligence in International Law, Second Report, page 23.

33. Due diligence generally refers to reasonable steps that governments can take to protect other states and peoples against threats that emanate from within their territory. It sets expectations to states to exercise due care under specified circumstances. However, it must be noted that due diligence is not one, but many standards of conduct in different circumstances, all premised on the idea that states ought to act and arguably also prevent transboundary harm arising from the use of ICTs.[107] By being an evolving principle of international law, it ought to be the basis of state behavior in circumstances where no more specific rules have been established. Even if one interprets recommendation (c) as an ICT-specific, non-binding, standard of due diligence, this does not mean that the very general principle of due diligence in its most generic form would not apply. The more specific manifestations of the obligation of due diligence compliment the general binding international law principle.

34. Even though states might be wary towards the application of recommendation (c) due to the fact that there is a feared burden the recommendation may impose, the general goal for recommendation (c) is to minimize transboundary harm and harmful cyber operations that are launched from or through states' territory.[108] The seemingly large burden imposed by recommendation (c) can be mitigated in several ways and due diligence in general leaves states the margin of appreciation to choose the ways or means by which to comply with the obligation.

Recommendations

35. State obligation of due diligence deriving from recommendation (c) is intrinsically linked to effective international cooperation.[109] Exchange of information is an

[107] ILA Study Group on Due Diligence in International Law, Second Report, page 47.
[108] Michael N. Schmitt, In Defense of Due Diligence, page 69.
[109] See commentary to recommendation (A).

essential facilitating element of effectively exercising due diligence. It covers inter alia the exchange of information about risks of significant transboundary harm with the potentially affected parties, potential threats in general, information about vulnerabilities, as well as sharing information for the investigation and prosecution purposes.[110] Therefore, establishing a system for requests of information sharing is of utmost importance.[111]

36. As to the specific measures that states have to take to mitigate transboundary harm deriving from the use if ICTs, recommendation (c) could be implemented by:

- Notifying and warning potential victims;[112]
- Using all means at a state's disposal to terminate the activity;[113]
- Investigating and punishing perpetrators.[114]

37. Cooperative "cyber diligence"[115] does not need to be limited to a state as actors in the international community. Public-private partnerships benefit states as agile private sector actors can help states mitigate incidents more effectively.[116] Global ICT companies can collaborate with states to proactively defend against attacks and remediate the impact of such

---

[110] Joanna Kulesza, op. cit., page 196. United Nations Doc A/48/10, p 24. See also Jason Healey, *The US Government and Zero-Day Vulnerabilities, Columbia Journal of International Affairs* (November 2016).

[111] See also commentary to recommendation (d) and recommendation (j).

[112] Corfu Channel case, pages 22-23. Arguably, the duty to warn may be extended to the duty to warn more generally other states of vulnerabilities detected in that other states or a third state's networks. Scott J. Shackelford, et al., Unpacking the International Law on Cybersecurity Due Diligence, page 9.

[113] Michael N. Schmitt, Tallinn Manual 2.0, page 48.

[114] Corfu Channel case, pages 19-20. British Claims in the Spanish Zone of Morocco case stated that due diligence requirement is also to prevent and punish the unlawful acts of armed groups, cf. vis-à-vis the activities of non-state actors in cyberspace. British Claims in the Spanish Zone of Morocco (1925), 2 RIAA 615, 2 3-6.

[115] Karine Bannelier-Christakis, op. cit., page 15.

[116] Contribution by Microsoft.

attacks.[117] In instances where private sector capabilities for identifying, preventing, detecting, responding to and recovering from incidents in cyberspace are on par if not better than those of certain states, pooling resources among states and private sector can enforce peace, security and stability.

38. Wingfield's contribution to this commentary proposed that the best place to start enforcing recommendation (c) is in the cases of cyber activities most strongly resembling transnational terrorism, i.e. the intentional targeting of civilians, civilian property and infrastructure for the purposes of making a political statement.[118] In this context, it is paramount for a state to analyse, which instances would in their opinion fall under activities that recommendation (c) should cover.

39. If the state accepts that the due diligence obligation includes also certain preventive actions,[119] then implementation of information security policies, implementation of national cybersecurity strategies, setting up CERTs, adopting appropriate domestic legislation for reporting vulnerabilities and incidents could serve as preventive measures taken under recommendation (c).[120] Enacting stringent national criminal laws against non-state actor activity on state's territory as well as for the commission of international acts within national boundaries can also be construed as a preventive measure. Complementing meaningful, detailed investigations into cyber attacks with prosecuting those who have engaged in malicious cyber attacks that have caused transboundary harm (non-state actors),[121] or in general imposing consequences on those who

---

[117] Microsoft, *From Articulation to Implementation: Enabling progress on cybersecurity norms*, (2016), page 8.

[118] Contribution by Thomas C. Wingfield.

[119] Contribution by Tang Lan also identified several preventive measures that States ought to take: "establish and improve related laws that can convict a crime, investigate, prosecute and penalize illegal cyber behaviour. At mechanism level, State should possess elementary capability of emergency response, including work force, organization and metrics."

[120] Michael N. Schmitt, Tallinn Manual 2.0, page 46.

[121] David E. Graham, Cyber Threats and the Law of War, Journal of National Security Law and Policy, Vol 4, 2010, pages 93-94. Jolley, Attribution,

perpetrate internationally wrongful acts (state actors), serve as stabilizing measures under recommendation (c).

40. Recommendation (c) is connected to harm and risk of such harm. Therefore, risk assessments and evaluation with regard to the facilitation of transnational harmful ICT activity need to be conducted. Focus in this case should also be on the procedure, i.e. how states conduct risk assessment. Whether a state has abided by its due diligence obligation is a determination done *ex post facto*. Therefore, from the perspective of the state, it is paramount to think through a procedure for assessing their due diligence obligations. What is the extent of obligations and what are the corresponding capabilities for mitigating known and potential threats? Communicating this to the international community helps to clarify specific standards that would fulfil the duty set out in recommendation (c) and create a certain level of expectations towards other states.

State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, page 227.

Recommendation 13 (d)

> *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. States may need to consider whether new measures need to be developed in this respect.*

Els De Busser

Contextualization

1. Recommendation (d) expresses the wish for efficient interstate cooperation in exchanging information and other forms of assistance for the purpose of investigation and prosecution of terrorist and criminal use of ICTs.

2. The matter addressed by recommendation (d) should be clearly distinguished from recommendation (a). First, both recommendations zoom in on the topic of cooperation; however, the purpose of the cooperation and the context in which cooperation takes place differ. Where recommendation (a) implies cooperation between states, the purpose is to maintain international peace and security. In this sense, the purpose of recommendation (a) is directly related to the United Nations Charter and the purposes of the United Nations expressed therein.[1] In general, threats to international peace and security have a different scope than that of criminal offences and terrorist activities. Even though overlap can exist when terrorist activities

[1] See also commentary on norm (a).

affect international security, terrorist activities can also be directed at national targets.[2] Recommendation (d) addresses the exchange of information and cooperation in the context of criminal offences and terrorist activities that can be directed at international targets or at national targets but have cross-border effects. The cross-border effects are related to the gathering of evidence for the purpose of criminal investigations and prosecutions or the surrendering of persons for the purpose of prosecution or execution of a sentence. Second, whereas recommendation (a) is predominantly—but not exclusively—addressing state actors, recommendation (d) is exclusively directed at non-state actors. This focus originates from the material scope of national criminal law that does not include offences committed by state actors.

3. This chapter has a strong emphasis on the EU due to the well-developed and detailed EU legal framework on information exchange and other cooperative mechanisms giving the EU member states, institutions and agencies relevant expertise in this field.

4. The norms and principles recommended in the 2013 United Nations GGE report included a reference to cooperation against criminal or terrorist use of ICTs. However the emphasis in 2013 was on intensifying cooperation on the one hand and harmonizing legal approaches on the other hand. The different emphases between the 2013 and the 2015 reports prompt two main comments. First, the current recommendation (d) does not mention an intensifying of existing cooperation, yet stresses the best way of cooperation. This should be understood as aiming for an efficient method of cooperation and exchange of information. Second, harmonization of legal approaches not only requires an extensive level of mutual trust among states, but also conflicts with national sovereignty that is particularly strong when criminal law is concerned. The significant difficulties that were met—and continue to be met—on the level of the EU when making efforts to harmonize substantive and procedural criminal law of the

[2] For example, the separatist Basque organization ETA in Spain and the Cellules Communistes Combattantes in Belgium during the 80s.

member states, demonstrate that this is an objective that should not be underestimated.[3]

5. Additionally, the 2013 recommendation limited its scope to law enforcement and prosecutorial agencies whereas recommendation (d) opens up its scope, referring to states without mentioning specific authorities or agencies. In practice, this distinction will not make a significant difference since the authorities involved in exchange of information and other forms of cooperation in criminal matters are mostly law enforcement and prosecutorial authorities. It should be noted however that administrative agencies can in certain states—and also on EU level[4]—play a substantial role in the cross-border exchange of information in criminal matters.[5]

6. It is essential to highlight that the context of (cross-border) criminal investigations and prosecutions is heavily dependent on the limits drawn by national law. Even the construction of the EU—which implies that the member states confer a significant part of their legislative competences to the EU institutions—does not allow for a full conferral of substantive and procedural criminal law to the EU.[6] Significant aspects such as the admissibility of evidence and the definition of a number of crimes thus remain a national competence.

7. The unmistakable and inherent connection of a national criminal justice system to the historical, political, cultural and religious identity of a state is the backdrop[7] for a recommendation

---

[3] See inter alia Valsamis Mitsilegas, *The Symbiotic Relationship Between Mutual Trust and Fundamental Rights in Europe's Area of Criminal Justice* (New Journal of European Criminal Law, 2015, Vol. 4), page 457 and Jannemieke Ouwerkerk, *Mutual Trust in the Area of Criminal Law*, in Hemme Battjes, Evelien Brouwer, et al, *The Principle of Mutual Trust in European Asylum, Migration, and Criminal Law* (Meijers Committee, Forum, 2011), pages 38-48.

[4] See f.e. the mandate of the EU anti-fraud agency OLAF in Regulation 883/2013, O.J. L 248, 18.09.2013, p. 1.

[5] Council of the EU, 6253/17, *Overview of the information exchange environment in the justice and home affairs area*, 15.02.2017.

[6] See Articles 82 and 83 TFEU.

[7] E. De Busser, *Big Data: The Conflict Between Protecting Privacy and Securing Nations*, in Atlantic Council and Thomson Reuters, *Report Big*

that zooms in on two concerns. Each of these concerns is divided in its turn over two types of criminal acts, each with their own specificities: 1) interstate exchange of information for the purpose of criminal use of ICTs on the one hand and terrorist use of ICTs on the other hand and 2) other forms of interstate cooperation for the purpose of criminal use of ICTs on the one hand and terrorist use of ICTs on the other hand. The distinction between the exchange of information and other cooperative measures has its origin in traditional mutual legal assistance in criminal matters.[8] Mutual legal assistance in criminal matters in the wider sense refers to all forms of interstate cooperation for the purpose of a criminal investigation or prosecution including extradition, exchange of information, other forms of cooperation—such as hearings by video- or teleconference, cross-border hot pursuit, controlled delivery and joint investigation teams—transfer of proceedings and transfer of sentences. Mutual legal assistance in criminal matters in the narrow sense focuses only on the exchange of information and the other forms of cooperation. For the purpose of this commentary, mutual legal assistance in criminal matters will be used in its narrow sense and will be divided in exchange of information on the one hand and the other forms of cooperation on the other.

8. Interstate cooperation and exchange of information in criminal matters—not in the least due to the aforementioned national scope of criminal laws—have their own challenges that are not necessarily related to the use of ICTs for criminal offences or terrorism. That specification will be made clear throughout this chapter.

9. As recommendation (d) refers to the threats of criminal or terrorist use of ICTs, it is necessary to clarify that this includes intelligence exchange in the field of national security as well as information exchange in the field of criminal law. Both areas are not always clearly separated and transfer of data from the field

Data: a Twenty-First Century Arms Race, June 2017, p. 6.

[8] See Council of Europe, Explanatory Report to the European Convention on Mutual Assistance in Criminal Matters, ETS No. 30, p. 2.

of national security into a criminal investigation is possible.[9] For the purposes of this chapter, the distinction between the two lies in the fact whether a suspicion of a concrete crime is present or not: when intelligence is concerned, no concrete suspicion is present whereas such suspicion is necessary for one to speak of the context of information exchange in criminal matters.

10. The question whether or not states need to consider developing new measures in the context of criminal or terrorist use of ICTs is a question that is not dealt with in the scope of this chapter, as this is an overarching question joining several other recommendations.[10] It will therefore not form part of the chapter on recommendation (d).

Background

11. The long tradition of mutual legal assistance in criminal matters originating from diplomatic traffic is embedded in a number of multilateral agreements and conventions and a large number of bilateral treaties or MLATs. The three most important multilateral agreements were concluded on the three largest levels of cooperation: the United Nations,[11] the Council of Europe[12] and the EU.[13] Apart from regional agreements with a smaller geographical scope—such as the Benelux[14] and the Nordic cooperation[15]—these are the most relevant legal bases for mutual legal assistance in criminal matters in practice. Their relevance is drawn from their wide geographical scope, as well as their wide material scope covering virtually all criminal offences and all

---

[9] Lorena Bachmaier Winter, *Section III Criminal Procedure, Information Society and Penal Law* (General Report, RIDP Vol. 85, 2014) page 78.

[10] Commentary by Anatoly A. Streltsov.

[11] United Nations Transnational Organised Crime Convention, 2000 (further: United Nations TOC).

[12] Council of Europe Convention on Mutual Legal Assistance in Criminal Matters, 1959, ETS No 30 (further: CoE MLA Convention).

[13] EU Convention on Mutual Legal Assistance in Criminal Matters, O.J. C 197, 12.7.2000, p. 3.

[14] Benelux Agreement on Cross-Border Police Cooperation, 2004, www.benelux.int/files/7713/9626/9329/BeneluxPolitieverdrag_8juni2004.pdf.

[15] Nordic Police Cooperation Agreement, 2002.

types of cooperation. In addition, the request-based cooperation stood the test of time due to its foundation on reciprocity besides allowing for a variety of grounds for refusal on the part of the requested state.

European Union

12. Aiming to speed up cross-border cooperation in criminal matters, the EU member states were introduced to the principle of mutual recognition as the cornerstone of such cooperation.[16] Rooted in the assumption of mutual trust and an endorsement of the same standards of human rights protection—embedded in the EU Charter of Fundamental Rights and Freedoms and the European Convention on Human Rights—mutual recognition offers member states less grounds for refusal of cooperation. For a list of 32 offences—including terrorism and computer-related crime—an assumption of dual criminality replaces the former check whether a particular behaviour constituted a criminal offence in both the requesting and the requested state. Ideally, mutual recognition measures—such as the European Arrest Warrant and the more recent European Investigation Order—would replace mutual legal assistance in criminal matters.

13. Since its introduction in practice with the European Arrest Warrant in 2002,[17] the mutual recognition principle wrestled with the presumed mutual trust among member states. Demonstrated in the jurisprudence of the Court of Justice of the EU,[18] member states do not have the same standards of human rights enforcement; hence trust among member states is not strong enough to ensure the undisturbed cooperation in criminal matters.

---

[16] Programme of measures to implement the principle of mutual recognition of decisions in criminal matters, O.J. C 12, 15.01.2001, page 10.

[17] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, O.J. L 190, 18.7.2002, page 1.

[18] CJEU, Joined Cases C-404/15 and C-659/15 PPU Pál Aranyosi and Robert Căldăraru, EU:C:2016:198. See also Bovend'Eerdt, K., (2016). The Joined Cases Aranyosi and Căldăraru: A New Limit to the Mutual Trust Presumption in the Area of Freedom, Security, and Justice?. Utrecht Journal of International and European Law. 32(83), pages 112–121.

Other EU initiatives for enhancing cooperation in criminal matters are less hindered by fundamental differences in human rights enforcement, but by difficulties in interpreting national law or by practical concerns using the—for mutual recognition measures typical—standardized formats.[19]

14. In the Stockholm Programme,[20] the European Council called on Europol to evolve and "become a hub for information exchange between the law enforcement authorities of the member states, a service provider and a platform for law enforcement services". Information exchange and intelligence analysis is the focal point of Europol's work and has been developed in the past years in order to improve police cooperation in the area of organized crime, terrorism and other forms of serious cross-border crime. In 2013, Europol established the EC3, the European Cybercrime Centre. Concentrating on forensics, strategy and operations related to cybercrime, EC3 offers operational and analytical support to member states' investigations. Due to lacking member states' efforts to feed Europol with the necessary information,[21] the new Europol Regulation[22] introduced an obligation for member state authorities to transfer relevant information to Europol. Even though genuine enforcement of such obligation is hardly possible, the significance of its inclusion in the Europol Regulation should not be underestimated.

15. As the judicial counterpart of Europol, Eurojust handles case-related information exchange between prosecutorial authorities. Since 2016, Eurojust has hosted the European Judicial Cybercrime Network[23] aiming to support prosecutors and judges

---

[19] For example the critiques on the use of the so-called Swedish Framework Decision that is designed to facilitate information and intelligence exchange between national law enforcement authorities: O.J. L 386, 29 December 2006, p. 89. See also Council of the EU, 9587/17, 23.5. 2017.

[20] O.J. C 115, 4 May 2010.

[21] Commission Staff Working Document Impact Assessment on adapting the European police Office's legal framework with the Lisbon Treaty, SWD(2013) 98 final, 27.3.2013, pages 8-13.

[22] On 1 May 2017, the Europol Regulation entered into force replacing the Europol Decision as the basic legal text.

[23] Council of the EU, Conclusions on the European Judicial Cybercrime Network, 10025/16, 9.6.2016.

dealing with cybercrime, cyber-enabled crime and investigations in cyberspace, as well as facilitating and enhancing cooperation between the competent authorities dealing with these offences.

Council of Europe and the United Nations

16. The objective and organization of the EU differs considerably from those of the Council of Europe (CoE) and the United Nations. Whereas the EU was established on the idea of an economic union, transferring legislative competences wholly or partially from the member states to a supranational institution, the CoE and the United Nations know no such transfer of competences. However, this does not mean that the lack of mutual trust among member states is not a factor in the cooperation within the CoE or the United Nations.

17. CoE and United Nations member states can rely on the aforementioned general conventions governing mutual assistance in criminal matters.[24] In addition, more specific conventions were concluded such as the CoE Cybercrime Convention and the United Nations Convention on the Suppression of Terrorist Bombings and the Convention for the Suppression of the Financing of Terrorism. Although these conventions were signed and ratified by a long list of member states, the absence of a few key players in the international field can stop cross-border cooperation in its tracks. Alternatively, bilateral MLATs can fill this gap.

18. Furthermore, ratification by member states does not necessarily imply a uniform or even similar application of the convention's provisions. For example, the CoE Cybercrime Convention's Chapter III on international cooperation is—similar to the CoE MLA Convention—based on offering assistance to the widest extent possible, however its material scope is limited to the crimes that are committed by use of a computer system, or where an ordinary crime not committed by use of a computer system involves electronic evidence.[25] Provisions on extradition, real-time collection of traffic data and interception of content data

[24] United Nations TOC and CoE MLA Convention and protocols.
[25] Cybercrime Convention, ETS No. 185, explanatory report, page 42.

can however be implemented by member states using a different scope.[26]

Analysis

19. Inspired by the wide material scope of norm (d), the commentators each focused on one or more specific sub-topics. The common themes are discussed here in subtitles covering two general subtitles zooming in on trust and fragmentation as issues that are at the core of interstate cooperation, and two more specific subtitles covering proaction and prevention on the one hand and evidence on the other focus on practical concerns that matter especially in the field of criminal use of ICTs.

Trust

20. Information sharing in general is often met with reluctance by states and their competent authorities. The reasons are not always clear. Some may think it would expose its intelligence sources and capability; some may be concerned to be breaching sensitive information, while others do not have competent capacity.[27] Divergent interests can be another reason.[28] Several commentators imply that trust is a prerequisite in the sharing of information.[29] The presence of a trust relationship among states that have an established cooperation in other areas will continue when cooperation in criminal matters is concerned. Smaller groups of states[30] and states having a common history or political ties—such as the aforementioned Benelux or Nordic Cooperation—tend to work together much easier towards a

[26] Ibid., p. 42. For example both Australia and Norway restrict assistance in real time collection of traffic data to serious offences but differ in defining the term "serious offences": Australia limits the scope to offences that are punishable by imprisonment for at least 3 years whereas Norway considers offences serious when punishable by imprisonment for a term of five years or more, or in case of a breach of specific penal provisions.

[27] Contribution by Tang Lan.

[28] Contribution by Thomas C. Wingfield.

[29] Contribution by Tang Lan.

[30] Contribution by Tang Lan and Thomas C. Wingfield.

common goal. This does not mean that the relationship of mutual trust is infallible. The aforementioned recent CJEU jurisprudence on mutual recognition and cooperation in criminal matters proves that cracks can appear in the ties between the members of a long-standing cooperative bond.

21. A long-established feature of interstate cooperation in criminal matters is the occurrence of informal cooperation. Such preference is equally related to trust, although this type of trust often plays on a more interpersonal level.[31]

22. On a proactive level, few initiatives prove that information sharing can equally be organized among allies, for example the US DHS' Automated Indicator Sharing (AIS) initiative. The AIS is a free platform enabling the sharing of cyber threat indicators between the US, the private sector[32] and other organizations. Israel[33] and Japan[34] have declared to join.[35] One commentator points out that when states can find a common goal such as ending child pornography on the Internet, cooperation will be significantly enhanced as all states can endorse such goal.[36] Building a climate of trust in sharing intelligence and information in the field of cybersecurity and incidents was touched upon by ENISA in their 2015 report on Cyber Security Information

---

[31] See. Saskia Hufnagel, *Policing Cooperation Across Borders* (Routledge 2016), pages 31-32 and Chantal Joubert and Hans Bevers, *Schengen Investigated* (Kluwer Law International, 1996), pages 27-29 and Detlef Nogala, *Policing Across A Dimorphous Border: Challenge and Innovation at the French-German Border* (9 *Eur. J. Crime Crim. L. & Crim Just.* 130, 2001), page 415.

[32] For example NEC: NEC Joins U.S. Department of Homeland Security; Initiative for Sharing Cyber Threat Indicators, Mar 15, 2017, http://www.nec.com/en/press/201703/global_20170315_01.html.

[33] Yonah Jeremy Bob, US Deputy of Homeland Security, *US-Israel to Sign Automated Cyber Information Sharing Agreement*, Jerusalem Post, Jun 20, 2016.

[34] Morgan Chalfant, *US, Japan deepen cyber information sharing*, May 4, 2017, http://thehill.com/policy/cybersecurity/331979-us- japan-deepen-cyber-information- sharing.

[35] Contribution by Tang Lan.

[36] Contribution by Thomas C. Wingfield.

Sharing[37] and resurfaces—besides economic incentives and incentives stemming from the quality, value and use of the information—in other reports as an incentive to information sharing.[38] A concrete example of a successful cooperation between two states was revealed in January 2018 when Dutch journalists published their research on how the Dutch intelligence services alerted the United States FBI and helped them avert intrusion of government networks by a group of hackers.[39]

Proaction and prevention

23. Cooperation in proaction and prevention with regard to terrorist and criminal use of ICTs is only implicitly included in norm (d), yet there is a clear trend among law enforcement and intelligence agencies to collect information at an earlier stage. This trend reaches further than only the terrorist and criminal use of ICTs and should be seen in the context of criminal investigations in general. Proaction and prevention can also be understood as a reliance on the relevant legal persons to implement and update appropriate safety and security measures, technical-human organization and risk assessments.[40] The latter is inspired by the goal of mitigating the impact of incidents or terrorist and criminal use of ICTs. Proaction and prevention will thus be covered here both in terms of the so-called "building of information positions" and in terms of appropriate safeguards by the relevant legal persons.

24. Building information positions originated from the field of intelligence-led policing and is slowly gaining traction as an approach. Intelligence-led-policing can be defined as a conceptual framework of conducting policing, as an information-organizing process that allows law enforcement agencies in their preventive

---

[37] ENISA, *Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches* (2015), pages 47-48.

[38] ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, 2010, pages 19-20 and ENISA, *Good Practice Guide Network Security Information Exchanges* (2009), page 17.

[39] Huib Modderkolk, *Hackers AIVD leverden cruciaal bewijs over Russische inmenging in Amerikaanse verkiezingen*, Volkskrant, 26.01.2018.

[40] Contribution by Lorenzo Picotti.

and repressive tasks, particularly state security issues, and fight against the most serious forms of crime, as terrorism and severe phenomena of transnational organized crime.[41]

25. It should be noted that the concept of building information positions means that the line between preventive and repressive crime fighting is blurred and, as a consequence, the field of preventive gathering of information by law enforcement authorities—for the purpose of a criminal investigation, not national security—is academically still underdeveloped.[42] This could explain why also in their national laws states are still working on drawing up legal frameworks for these practices. The 2014 AIDP report on information society and penal law drawing on a comparative exercise of country reports, emphasized that the lack of a clear distinction between the preventive and the repressive sphere hinders a transparent defining of law enforcement powers in building information positions.[43] Hence, interstate cooperation can be affected by this lack of clarity.

26. Efficient cooperation and information exchange is of vital importance for the early detection of terrorist and criminal use of ICTs, in particular when these are of a cross-border nature. On the law enforcement side, a new proposal on setting up an EU Law Enforcement Emergency Response Protocol (LEERP) is intended to be an instrument supporting the member states' law enforcement authorities in addressing transnational cyber-attacks through a fast and effective sharing of relevant information and coordination of investigations.[44] On the information security side, networks of national CERTs and CSIRTs—such as FIRST,[45]

---

[41] Lorena Bachmaier Winter, op. cit., pages 89-90. See also UNODC Handbook on the Crime Prevention Guidelines: Making them Work, 2010, https://www.unodc.org/pdf/criminal_justice/Handbook_on_Crime_Prevention_Guidelines_-_Making_them_work.pdf.

[42] Lorena Bachmaier Winter, op. cit., page 92.

[43] Ibid., p. 94.

[44] Council of the EU, Improving the EU's fight against cybercrime: EU law enforcement response—Progress report, 15738/17, 13.12.2017, p. 4.

[45] FIRST is an international confederation of trusted computer incident response teams who cooperate in handling computer security incidents and promote incident prevention programs. See https://www.first.org.

AP-CERT[46] and the EU CSIRTs Network—ensure an exchange of best practices and mutual assistance among their members.[47] ENISA concluded based on a survey among European and selected non-European CERTs that the proactive detection of incidents is used only to a limited extent compared to reactive actions. Moreover, the survey showed that respondents were not satisfied with their sources of information.[48] The verification of the quality of information sharing in the context of terrorist and criminal use of ICTs is linked to the chain of evidence and will therefore be touched upon in the subtitle "evidence".

27. Ensuring the appropriate safeguards are in place with the relevant legal persons is an objective that is often associated only with unlawful disclosures of data. However, the lack of adequate security standards can considerably facilitate terrorist and criminal use of ICTs. For that reason, states should ensure that legal persons who manage data in cyberspace adopt, having regard to the state of the art, appropriate technical and organizational security measures to prevent unlawful destruction, loss, alteration, unauthorized disclosure or access to data and to minimize the impact of incidents affecting the security of network and information systems.[49]

Fragmentation

28. In the context of international cooperation in criminal matters, fragmentation can occur not only on the level of applicable laws, but also on the level of the threat. Fragmentation in laws refers to the lack of a uniformly applicable law for a large number of states, region or continent. Fragmentation regarding the threat refers to a variety in types of threats rather than the occurrence of an identical threat for a large number of states, region or continent.

---

[46] Asia Pacific Computer Emergency Response Team. See http://www.apcert.org.

[47] Contribution by Tang Lan.

[48] ENISA, *Proactive Detection of Network Security Incidents*, p. 133.

[49] Contribution by Lorenzo Picotti.

29. With criminal law and law enforcement in principle having a national scope and privacy and data protection laws demonstrating significant local and regional differences, cross-border cooperation risks being hampered by conflicting laws. Information received from one country may be inadmissible as evidence in the trial organized by another country on grounds of privacy violation or breaches of fundamental procedural provisions.[50] The 2010 EU–United States Agreement on exchanging financial messaging data for the purpose of the Terrorist Finance Tracking Program[51] is an example of an ad hoc agreement designed to overcome such differences. The recent Microsoft versus United States case[52] demonstrated that the issue is still more than just theoretical. To this date, the OECD is the only forum that included this concern in non-binding guidelines urging states to work toward their own solutions by identifying factors indicating one applicable law or making a distinct choice for the law offering the best data protection.[53]

30. Fragmentation in laws raises the question of jurisdiction—and the extraterritorial reach of a warrant—when a provider of email services stores data abroad. The question was at the heart of a legal battle between Microsoft and the United States government when a probable cause warrant was issued for email account data stored on an Irish server. After the invalidation of the warrant in appeal by the Second Circuit,[54] the United States Department of Justice turned to the Supreme Court, who will hear the parties on 27 February 2018 and is expected to rule on the case later in 2018. Jennifer Daskal stressed the consequence of applying territorial-based rules onto unterritorial data: since such an approach would

[50] E. De Busser, "op. cit., p. 13-15.

[51] O.J. L 195, 27.7.2010.

[52] US Court of Appeals for the Second Circuit, No. 14-2985, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation.

[53] OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013, "Explanatory Memorandum," http://www.oecd.org/sti/ieconomy/privacy.htm.

[54] US Court of Appeals for the Second Circuit, No. 14-2985, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation.

fail to reflect the unique features of data, it would likely fuel data localization movements, which in turn would undercut the overall efficiency of the Internet.[55] In addition to the question of fragmentation, the broader ICT community in all states would benefit from a deeper, clearer understanding of the principles of extraterritorial jurisdiction under international law.[56]

31. When threats involving the use of ICTs are concerned, the most recent Europol IOCTA report[57] shows a clear difference in threats per region. Whereas the threats are clearly more homogenous in the African countries and the Americas—involving three, respectively two types of threats—the opposite is true for Europe and Asia. It is necessary to point out that when zooming in on one particular country, for example the United Kingdom, the threats show more homogeneity.

32. Fragmentation in laws acting as an obstacle for effective cooperation is a difficulty that can be overcome by concluding methods of cooperation, even when mutual trust is an often hard-to-realize prerequisite. In addition, fragmentation in threats could further affect initiatives of information exchange and cooperation in criminal matters, keeping in mind the reciprocal nature of mutual assistance and the diverse interests of states.[58]

Evidence

33. The availability of a variety of data—personal and non-personal—in the online environment introduced new questions for law enforcement authorities finding material that could function as evidence in a later criminal trial. In particular for terrorist and criminal use of ICTs, a large part of the evidence will have a digital origin. This raises two issues: accessibility of the data and verifiability of the data.

---

[55] Jennifer Daskal, *The Un-Territoriality of Data* (Yale Law Journal, 2015, Vol. 125), p. 397.

[56] Contribution by Thomas C. Wingfield.

[57] Europol, Internet Organized Crime Threat Assessment, 2017, p. 66-71, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017.

[58] Contribution by Thomas C. Wingfield.

34. The accessibility of data that is necessary for the purpose of a criminal investigation can be obstructed by the use of encryption technologies by offenders. Encryption technologies are a typical dual-use technology and can be utilized by law-abiding data subjects concerned about the privacy of their communications or other data. Yet, offenders aiming to shield the data linking them to a crime can also use them, making the breaking into encrypted files the new challenge for law enforcement. The debate on whether or not to require manufacturers to build in so-called backdoors in encryption software is held on an academic, law enforcement, as well as a political level. Also here, governments have taken different stands. Where the Netherlands has taken a clear position against the building in of vulnerabilities in software,[59] France and Germany lean towards the opposite view.[60]

35. Myriam Dunn Cavelty commented on the risks of intentional vulnerabilities: "Strategic exploitation of vulnerabilities in computer systems and the weakening of encryption standards have the potential to destroy trust and confidence in cyberspace overall, which would be a disaster from an economic perspective. Neither is there any guarantee that an intelligence actor who has acquired knowledge about an exploitable vulnerability has full control over it and/or can keep it secret. Capabilities in cyberspace are a derivative of knowledge. Hence, they can just as well be identified and exploited by criminal hackers or even 'terrorists'."[61]

36. In October 2017, the European Commission announced its eleventh progress report towards an effective and genuine Security Union.[62] Dedicating a significant part of this agenda to the issue of encryption and recognizing its importance for cybersecurity, the Commission proposed—after discussion with

[59] Letter by the Ministers of Security and Justice and Economic Affairs to the President of the House of Representatives, nr. 26643-383, 04.01.2016: https://www.tweedekamer.nl/kamerstukken/brieven _regering/detail?id=2016Z00009&did=2016D00015.

[60] Catherine Stupp, EU to propose new rules targeting encrypted apps in June, Euractiv, 29.03.2017, https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/.

[61] Contribution by Myriam Dunn Cavelty.

[62] European Commission, COM(2017) 608 final, p. 8–10.

the member states and relevant stakeholders—a set of measures supporting law enforcement and judicial authorities in their work. The proposal announces a legal framework for cross-border access to—not encrypted—electronic evidence in early 2018. Aiming to steer clear of prohibiting, limiting or weakening encryption, the Commission proposes a range of measures to support Member State authorities, including (financial) support for Europol in its decryption capability.

37. Even when the concrete proposals are at this moment not yet public, the EU clearly favours a direction that fits the historical objective of the EU, namely protecting the economic union by not requiring planned vulnerabilities. Similar to seeking the balance between protecting its citizens' human rights and at the same time ensuring effective cross-border law enforcement—the idea behind the area of freedom, security and justice—the EU's position aims to keep ICTs secure.

38. The verification of the quality of incoming information plays a significant role in all evidence-gathering activities. Information is not admissible as evidence in a trial if doubts could be raised regarding its accuracy. When (digital) data are concerned relating to terrorist or criminal use of ICTs, the correctness of identification of incidents is crucial for ruling out the potential duplication of data, false positives and the implications of data aging.[63] The adoption of common standards for the exchange of incident information was therefore a recommendation expressed by ENISA in this respect.[64] Similar to Europol's 4x4 evaluation system used for assessing the reliability of the information and the reliability of the source of the information,[65] a set of evaluation codes could be developed for information exchange on the terrorist or criminal use of ICTs.

---

[63] ENISA, Proactive Detection of Network Security Incidents, p. 128-131.
[64] Ibid., p. 132.
[65] Article 9 of the Agreement between Europol and Interpol, 2001.

Recommendations

39. Cooperation between states in the context of terrorist or criminal use of ICTs should preferably be organized on a small geographical scope involving trusted states.

Since trust between cooperating states is necessary for an efficient exchange of information, organizing such cooperative frameworks on a smaller scale between fewer trusted partners is a more effective method in comparison to geographically larger cooperative frameworks. Mutual trust as a prerequisite for "blind" cooperation between states has proven to be too difficult in practice to achieve.

40. On a national level, a clear definition of law enforcement powers in building information positions is necessary.

By defining the line between proactive and preventive information gathering on the one hand and repressive crime fighting on the other hand, national authorities should bring more transparency in the lawful gathering of information for the purpose of investigations and prosecutions of terrorist and criminal use of ICTs.

41. Define a method for the verification of the quality of information.

When gathering information and exchanging information on the purpose of investigations and prosecutions of terrorist and criminal use of ICTs, law enforcement authorities would benefit from using appropriate methods for verifying the quality of information.

42. States should invest in the decryption capabilities of their law enforcement authorities rather than require the installing of intentional vulnerabilities in software.

Safeguarding the security of communication but at the same time allowing law enforcement authorities to gather information for the purpose of investigations and prosecutions of terrorist and criminal use of ICTs, encryption software should not be weakened. The preferred approach is to enhance the decryption capabilities of the law enforcement authorities.

Recommendation 13 (e)

> *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 General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.*

Barrie Sander

Contextualization

1. The recommendation in paragraph 13 (e) of the United Nations GGE 2015 Report calls upon States to guarantee full respect for human rights in ensuring the secure use of information and communications technologies (ICTs). Despite its broad framing, the scope of the recommendation is restricted to calling upon States to respect four human rights resolutions in particular: Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, and General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age.

2. The resolutions referred to in paragraph 13 (e) direct the attention of States towards the following issues concerning the relationship between human rights and ICTs:

- Affirming that the same rights that people have offline must also be protected online;[1]
- Recognizing the global and open nature of the Internet and the rapid advancement in ICTs as a driving force in accelerating progress towards development in its various forms;[2]
- Ensuring respect for and the protection of the right to privacy, including in the context of digital communication, and taking measures to put an end to violations of the right and to create the conditions to prevent such violations;[3]
- Reviewing procedures, practices and legislation concerning surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a review to upholding the right to privacy;[4]
- Establishing or maintaining existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;[5]
- Providing individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access

---

[1] *The promotion, protection and enjoyment of human rights on the Internet*, Human Rights Council Resolution 20/8 of 16 July 2012 (A/HRC/RES/20/8), para. 1; *The promotion, protection and enjoyment of human rights on the Internet*, Human Rights Council Resolution 26/13 of 14 July 2014 (A/HRC/RES/26/13), para. 1; *The right to privacy in the digital age*, A/RES/68/167 of 18 December 2013 (A/RES/68/167), para. 3; *The right to privacy in the digital age*, A/RES/69/166 of 18 December 2014 (A/RES/69/166), para. 3.

[2] A/HRC/RES/20/8, para. 2; A/HRC/RES/26/13, para. 2; A/RES/68/167, para. 2; A/RES/69/166, para. 2.

[3] A/RES/68/167, para. 1 and 4(a)-(b); A/RES/69/166, para. 1 and 4(a)-(b).

[4] A/RES/68/167, para. 4(c); A/RES/69/166, para. 4(c).

[5] A/RES/68/167, para. 4(d); A/RES/69/166, para. 4(d).

to an effective remedy, consistent with international human rights obligations;[6]

- Ensuring respect for and the protection of the right to freedom of expression online;[7]
- Combating advocacy of hatred that constitutes incitement to discrimination or violence on the Internet, including by promoting tolerance and dialogue;[8]
- Addressing security concerns on the Internet in accordance with international human rights obligations, including through national democratic, transparent institutions, based on the rule of law; and[9]
- Promoting and facilitating access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries,[10] including through the promotion of digital literacy,[11] as well as the formulation and adoption of national Internet-related public policies that have the objective of universal access and enjoyment of human rights at their core.[12]

3. While it may be queried whether all aspects of these thematic areas fall *directly* within the scope of the mandate of the United Nations GGE,[13] this commentary will provide general guidance with respect to each of them in accordance with the ordinary meaning of the text of paragraph 13 (e).

4. In terms of the general purpose of recommendation (e), it is possible to identify at least two links between the norm and

---

[6] A/RES/69/166 (2014), at A/RES/69/166 (2014), para. 4(e).
[7] A/HRC/20/8, para. 1; and A/HRC/26/13, para. 1.
[8] A/HRC/26/13, para. 6.
[9] A/HRC/26/13, para. 5.
[10] A/HRC/20/8, para. 3; and A/HRC/26/13, para. 3.
[11] A/HRC/26/13, para. 4.
[12] A/HRC/26/13, para. 7.
[13] Pursuant to A/RES/56/19, the mandate of the United Nations GGE is restricted to considering "existing and potential threats in sphere of information security and possible cooperative measures to address them".

the existing and emerging cyber threats expressly identified within the GGE Reports: first, the recommendation may be understood as a call for States to ensure that the means they use to address the various malicious uses of ICTs by State and non-State actors—including cyber attacks on critical infrastructure,[14] vulnerabilities in the ICT supply chain,[15] cyber terrorism,[16] and cyber crime[17]—are in accordance with human rights; and second, by calling for the promotion and facilitation of universal access to the Internet,[18] the recommendation is at least implicitly concerned with addressing the threat posed by different levels of capacity for ICT security among different States, which has been deemed by the GGE to increase vulnerability across the global network.[19]

5. It is also important to note at the outset that the human rights emphasis is related to some of the other recommendations set out in the GGE Reports. In particular, the call to promote and facilitate universal access to the Internet is complemented by various recommendations put forward by the GGE to enhance capacity building in the area of ICT security.[20] In addition, the proposed norm is complemented by the GGE's recognition that international law applies to the use of ICTs by States.[21] More specifically, the GGE has recognised that, in their use of ICTs, as well as their efforts to address the security of ICTs, "States

[14] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174), para. 5; *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98), para. 9; *roup of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 30 July 2010 (A/65/201), para. 9.

[15] A/68/98, para. 8; A/65/201, para. 10.

[16] A/70/174, para. 6; A/68/98, para. 7; A/65/201, para. 6.

[17] A/70/174, para. 7; A/65/201, para. 5 and 8.

[18] A/HRC/20/8, para. 3; A/HRC/26/13, para. 3, 4 and 7.

[19] A/70/174, para. 11; A/68/98, para. 10; A/65/201, para. 6.

[20] A/70/174, para. 19-23; A/68/98, para. 30-33; A/65/201, para. 17.

[21] A/70/174, para. 24; A/68/98, para. 19.

must comply with their obligations under international law to respect and protect human rights and fundamental freedoms".[22]

Background

6. The human rights recommendation in the GGE 2015 Report was preceded by a number of statements issued by States in the context of the United Nations General Assembly's First Committee, cyber incidents that focused the attention of the international community on the relationship between human rights and ICTs, and a range of normative materials issued both within and beyond the United Nations system.

7. Prior to the proposal of the human rights recommendation in the GGE 2015 Report, several States referred to the relationship between human rights and the use of ICTs within the United Nations General Assembly's First Committee.[23] In particular, a number of states confirmed that the use of ICTs may pose a threat to human rights,[24] and affirmed that states should use and prevent the abuse of ICTs in a manner consistent with respect for human rights.[25] Some states also referred to particular

---

[22] A/70/174, para. 28 (b). See also, A/70/174, para. 26 ("In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: […] respect for human rights and fundamental freedoms;"); and A/68/98, para. 21 ("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").

[23] In general terms see, for example, *Developments in the Field of Information and Telecommunications in the Context of International Security,* Report of the Secretary-General, A/58/373, 17 September 2003, at 10 (Russian Federation) and 15-17 (Ukraine).

[24] See, for example, *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, at 8-9 (Russian Federation); *and Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, A/68/156, at 10 (Ukraine).

[25] See, for example, *Developments in the Field of Information and Telecommunications in the Context of International Security,* Report of

domestic and regional regulations related to the protection of human rights in the context of using ICTs.[26] The importance

---

the Secretary-General, A/55/140, 10 July 2000, at 4 (Russian Federation); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, Addendum, A/61/161/Add.1, 31 October 2006, at 2 (Mexico); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, A/64/129, 8 July 2009, at 6 (Kazakhstan); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, Addendum, A/64/129/Add.1, 9 September 2009, at 9 (Spain); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, Addendum, A/66/152, 15 July 2011, at 3 (Australia) and 13 (The Netherlands); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, A/67/167, 23 July 2012, at 16 (Ukraine); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, Addendum, A/68/156/Add.1, 9 September 2013, at 4 (Canada); and *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, A/69/112, 30 June 2014, at 3 (Austria).

[26] See, for example, *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, Addendum, A/55/140/Add.1, 3 October 2000, at 3 (Poland referring to domestic regulations for data-processing and the rights of the individuals whose data are processed); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, A/57/166, 2 July 2002, at 3 (Guatemala referring to the right to freedom of thought and expression enshrined in Article 13 of the American Convention on Human Rights); and *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, A/62/98, 2 July 2007, at 6 (Burkina Faso referring to domestic regulations protecting the privacy of individuals in the context of the processing of personal data); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, Addendum, A/64/129/Add.1, 9 September 2009, at 10-11 (Spain referring to domestic regulations protecting personal data and the right to privacy); *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, A/65/154, 20 July 2010, at 7 (Mexico referring to domestic regulations concerning the protection of personal data and the right to access, correct and delete such data); and *Developments in the Field of Information and*

of respecting human rights and fundamental freedoms in the use of ICTs was also referred to in the preambular paragraphs of a number of United Nations General Assembly resolutions adopted based on the work of the First Committee.[27]

8. Beneath the surface of these general statements affirming the importance of respecting human rights online, a division of emphasis is discernible between different States. On the one hand, whilst affirming the importance of ensuring respect for human rights, some States have placed emphasis on such respect being premised on compliance with relevant national laws and regulations. For instance, in a letter to the United Nations Secretary-General in 2011, Russia, China, Tajikistan and Uzbekistan proposed an international code of conduct for "information security", which included a call for States "[t]o fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations".[28] In a similar vein, Iran has stated that the

---

Telecommunications in the Context of International Security, Report of the Secretary-General, Addendum, A/66/152/Add.1, 16 September 2011, at 6 (Portugal referring to domestic regulations protecting freedom of information, privacy and data protection, and copyright protection).

[27] See, for example, *Developments in the field of information and telecommunications in the context of international security*, Resolution 68/243 of 27 December 2013(A/RES/68/243); *Developments in the field of information and telecommunications in the context of international security*, Resolution 69/28 of 2 December 2014 (A/RES/69/28). Subsequent to the A/70/174, see also, *Developments in the field of information and telecommunications in the context of international security*, Resolution 70/237 of 23 December 2015 (A/RES/70/237); and *Developments in the field of information and telecommunications in the context of international security*, Resolution 71/28 of 9 December 2016 (A/RES/71/28).

[28] '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, at 4. Notably, however, this restrictive wording was replaced with wording drawn from Article 19 of the International Covenant on Civil and Political Rights in a more recent proposal of an international code of conduct for "information security": 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the

right to freedom of expression "in no case, should be exercised contrary to the purposes and principles of the United Nations, national laws and the principles of protection of national security, public order, public health or morals and decency".[29]

9. By contrast, a number of other States have placed greater emphasis on the principle of free flow of information.[30] For instance, the United Kingdom has declined to recognise the validity of the term "information security" to the extent that "it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".[31] In a similar vein, the United States has placed particular emphasis on ensuring that the implementation of security measures does not impinge upon the freedom of any individual to seek, receive and impart information and ideas through any media and regardless of frontiers.[32] In line with this perspective, the Netherlands has made specific reference to its initiation of the Freedom Online Coalition, a group comprised of like-minded States committed to "promoting Internet freedom and to stressing the importance of digital rights", as well as working with civil society and the private sector in a multi-stakeholder process to "support the ability of individuals to exercise their human rights and fundamental freedoms online".[33]

Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General', A/69/723, 13 January 2015, at 5.

[29] On Internet freedom and human rights, see generally, Daniel Joyce, *Internet Freedom and Human Rights* (26 *European Journal of International Law,* 2015), page 493.

[30] A/68/156/Add.1, page 13 (Iran).

[31] A/68/156, page 15 (United Kingdom). See similarly, A/69/112/Add.1, page 3 (France).

[32] A/59/116/Add.1, page 3 (United States of America referring to Article 19 of the Universal Declaration of Human Rights). See similarly, A/66/152, pages 19-20 (United States of America).

[33] A/68/156/Add.1, page 17 (The Netherlands). See similarly, A/69/112/Add.1, page 6 (Sweden emphasizing "the need to maintain a human rights and multi-stakeholder perspective when addressing information and communication technologies and international security").

10. Recommendation (e) in the GGE 2015 Report was also proposed against the backdrop of a number of cyber incidents, which garnered increasing attention around the relationship between human rights and ICTs.[34] Particularly notable were the disclosures facilitated by Edward Snowden in 2013 through WikiLeaks and media entities such as *The Guardian* and *The New York Times*. The Snowden disclosures exposed the global surveillance activities of a number of States, most notably those of the so-called "Five Eyes" intelligence alliance, comprising the United States, the United Kingdom, Canada, Australia and New Zealand. The disclosed surveillance programmes were revealed to have targeted a wide range of State and non-State actors, including officials of international organisations, State organs (including heads of State), companies, non-governmental organisations, and individuals suspected of involvement in international terrorism.[35]

11. Although human rights concerns about government surveillance long predate the Snowden disclosures, these revelations pushed the issue to the forefront of the international agenda.[36] In particular, at the opening of the United Nations General Assembly's 68th Session on 24 September 2013, then-Brazilian President Dilma Rousseff delivered a speech that expressly characterised the cyber surveillance activities as a "grave violation of human rights and of civil liberties".[37]

---

[34] For a detailed account of the relationship between human rights and ICTs, which discusses a range of cyber incidents, see generally Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer, 2017), at 45-152 and 241-260.

[35] For an overview of the Snowden disclosures, see generally, Ewen MacAskill and Gabrial Dance, *NSA Files: Decoded, What The Revelations Mean For You* (The Guardian, 1 November 2013).

[36] See similarly, Carly Nyst and Tomaso Falchetta, *The Right to Privacy in the Digital Age* (9 *Journal of Human Rights Practice,* 2017), page 107; and Dinah PoKempner., *Cyberspace and State Obligations in the Area of Human Rights*, in Katharina. Ziolkowski, (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO Cooperative Cyber Defence Centre of Excellence, 2013), page 253.

[37] 'Statement by Dilma Rousseff at the Opening of the General Debate of the Sixty-Eighth Session of the United Nations General Assembly', New

Subsequently, in November 2013, Brazil and Germany introduced a draft resolution in the United Nations General Assembly's Third Committee entitled, "The Right to Privacy in the Digital Age".[38] On 18 December 2013, a revised version of the resolution was adopted without a vote by the General Assembly as Resolution 68/167.[39] It is this resolution and its successor, General Assembly Resolution 69/166,[40] which are expressly referred to within the human rights norm proposed in the GGE 2015 Report.

12. In terms of normative materials, recommendation (e) may be situated within the framework of international human rights law, a body of law that derives from a range of sources including:[41] the Universal Declaration of Human Rights; international treaties, such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR); regional treaties, such as the European Convention on Human Rights, the American Convention on Human Rights, and the African Charter on Human and Peoples' Rights; the large body of jurisprudence that has been delivered by regional human rights courts; the General Comments of the Human Rights Committee, the treaty body that monitors the implementation of the ICCPR; the reports of United Nations Special Rapporteurs; United Nations General Assembly and Human Rights Council resolutions; statements of non-official expert bodies, including the Johannesburg Principles on National Security, and the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights; and domestic legislation and judicial decisions.

13. In terms of materials specifically focused on the relationship between human rights and ICTs, the human rights

---

York, 24 September 2013, accessible online at: https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

38 United Nations General Assembly Draft Resolution, 'The Right to Privacy in the Digital Age', 1 November 2013, A/C.3/68/L.45.

39 A/RES/68/167.

40 A/RES/69/166.

41 Dinah PoKempner, op. cit., page 243-244.

norm was preceded by a range of normative instruments and reports both within and beyond the United Nations system. Within the United Nations system, a number of resolutions of the United Nations General Assembly and the Human Rights Council examined ICTs and freedom of opinion and expression,[42] ICTs and the right to privacy,[43] ICTs and development,[44] and the promotion, protection and enjoyment of human rights on the Internet.[45] Beyond resolutions, the Human Rights Committee also examined the interaction between ICTs and human rights in General Comment No. 16 on the right to privacy and General Comment No. 34 on freedom of opinion and expression,[46] though it has been noted that the former is in

---

[42] See, for example, A/HRC/12/16, *Freedom of Opinion and Expression*, 2 October 2009, A/HRC/RES/12/16; and A/HRC/23/2, *The Role of Freedom of Opinion and Expression in Women's Empowerment*, 13 June 2013, A/HRC/RES/23/2.

[43] See, for example, A/RES/68/167, A/RES/69/166, A/HRC/RES/28/16. Subsequent to A/70/174, see also A/RES/71/199.

[44] See, for example, *Information and Communication Technologies for Development*, United Nations A/RES/66/184 of 22 December 2011, (A/RES/66/184); *Information and Communication Technologies for Development*, United Nations A/RES/68/198 of 20 December 2013 (A/RES/68/198); *Information and Communication Technologies for Development*, United Nations A/RES/69/204 of 19 December 2014, (A/RES/69/204). Subsequent to A/70/174, see also, Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society, United Nations A/RES/70/125 of 16 December 2015 (A/RES/70/125); *Information and Communication Technologies for Development*, United Nations A/RES/70/184 of 22 December 2015 (A/RES/70/184); *Information and Communication Technologies for Development*, United Nations A/RES/71/212 of 21 December 2016 (A/RES/71/212).

[45] See, for example, A/HRC/20/8 and A/HRC/26/13. Subsequent to A/70/174, see also The Promotion, Protection and Enjoyment of Human Rights on the Internet, Human Rights Commission Resolution 32/13 of 1 July 2016 (A/HRC/RES/32/13); and *Rights of the Child: Information and Communications Technologies and Child Sexual Exploitation* Human Rights Committee Resolution 31/7 of 23 March 2016 (A/HRC/RES/31/7).

[46] Human Rights Committee, 'General Comment No. 16—Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I); and Human Rights Committee, 'General Comment No.

need of updating in light of technological developments over the course of the past two decades.[47]

14. A number of important reports on various aspects of the relationship between human rights and ICTs were also published by United Nations Special Rapporteurs. In particular, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression published reports concerning access to online content and access to an Internet connection,[48] hate speech,[49] as well as the implications of State surveillance of communications on the exercise of the rights to privacy and to freedom of opinion and expression.[50] In addition, the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism produced reports on the erosion of the right to privacy by counter-terrorism policies, including the use of mass digital surveillance and bulk access technology.[51] Following the GGE 2015 Report, the relationship between human rights and ICTs has continued to form a focal

---

34—Freedom of Opinion and Expression', ICCPR 12 September 2011, Document CCPR/C/GC/34.

47 'Report of the United Nations Special Rapporteur on the Promotion and Enjoyment of the Right to Freedom of Opinion and Expression', 17 April 2013 (A/HRC/23/40), para. 98.

48 *Report of the United Nations Special Rapporteur on the Promotion and Enjoyment of the Right to Freedom of Opinion and Expression*, 16 May 2011, A/HRC/17/27; and *Report of the United Nations Special Rapporteur on the Promotion and Enjoyment of the Right to Freedom of Opinion and Expression*, 10 August 2011, A/66/290.

49 *Report of the United Nations Special Rapporteur on the Promotion and Enjoyment of the Right to Freedom of Opinion and Expression*, 7 September 2012, A/67/357.

50 *Report of the United Nations Special Rapporteur on the Promotion and Enjoyment of the Right to Freedom of Opinion and Expression*, 17 April 2013, A./HRC/23/40.

51 *Report of the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, 28 December 2009, A/HRC/13/37; and *Report of the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, 23 September 2014, A/69/397.

point in the reports of these Special Rapporteurs,[52] as well as the newly established United Nations Special Rapporteur on the Right to Privacy.[53]

15. Beyond the reports of United Nations Special Rapporteurs, the United Nations Counter-Terrorism Implementation Task Force,[54] the United Nations Office on Drugs and Crime,[55] the Office of the United Nations High Commissioner for Human Rights,[56] as well as the International Telecommunications Union[57] also examined various security-related dimensions of

---

[52] See, in particular, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, 29 April 2016, A/HRC/31/65 (examining how to counter violent extremism); *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 22 May 2015, A/HRC/29/32 (examining encryption); *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 11 May 2016, A/HRC/32/38 (examining the private sector in the digital age); and *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 30 March 2017, A/HRC/35/22 (examining digital access providers).

[53] *Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci*, 8 March 2016, A/HRC/31/64; *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 11 May 2016, A/HRC/32/38; *Report of the Special Rapporteur on the Right to Privacy*, 24 February 2017, A/HRC/34/60; and *Report of the Special Rapporteur on the Right to Privacy*, 19 October 2017, A/72/43103.

[54] Counter-Terrorism Implementation Task Force, *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes* (CTITF Publication Series, February 2009); and Counter-Terrorism Implementation Task Force, *Countering the Use of the Internet for Terrorist Purposes—Legal and Technical Aspects* (CTITF Publication Series, May 2011).

[55] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (United Nations, 2012); and United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (Draft, February 2013).

[56] *Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age*, 30 June 2014, A/HRC/27/37.

[57] International Telecommunications Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (November 2014).

the relationship between human rights and ICTs prior to the proposal of the human rights norm.

16. Outside the United Nations system, the recommendation in question was preceded by a range of multi-stakeholder, intergovernmental, private industry, and civil society initiatives:

- At the multi-stakeholder level, the Multi-Stakeholder Statement from the Global Multi-Stakeholder Meeting on the Future of Internet Governance ("NETmundial") in April 2014 expressly acknowledged the need for human rights to underpin Internet governance.[58]
- At the intergovernmental level, in July 2013, the Organisation for Economic Co-operation and Development produced a set of guidelines governing the protection of privacy and transborder flows of personal data.[59]
- With respect to private industry, a range of initiatives formulated non-binding principles on freedom of expression and privacy, including the Telecommunications Industry Dialogue on Freedom of Expression and Privacy,[60] as well as the Global Network Initiative.[61]
- In addition, civil society groups facilitated the production of sets of non-binding principles concerning particular dimensions of the relationship between human rights and

[58] NETmundial Multistakeholder Statement, 24 April 2014.

[59] Organisation for Economic Co-operation and *Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL as amended on 11 July 2013 by C(2013)79, Annex (2013). Subsequent to the A/70/174, see also, G7 *Declaration on Responsible States Behavior in Cyberspace*, Lucca, 11 April 2017; and G7, *Principles and Actions on Cyber, endorsed in Ise-Shima*, 26 and 27 May 2016.

[60] Telecommunications Industry Dialogue on Freedom of Expression and Privacy, *Guiding Principles* (March 2013).

[61] Global Network Initiative, *Principles on Freedom of Expression and Privacy* (October, 2008).

ICTs, including the right to information and the application of human rights to communications surveillance.[62]

- Subsequent to the GGE 2015 Report, in 2016, the World Bank's *World Development Report* and the Global Commission on Internet Governance's *One Internet* report each examined issues relating to improving access to the Internet.[63] In addition, in 2017, a group of 19 international law experts published the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, extending the coverage of the first edition of the manual to the international law governing cyber warfare to peacetime legal regimes, including international human rights law.[64]
- Finally, the human rights recommendation was also preceded by a range of domestic and regional jurisprudence and legislation concerning the relationship between human rights and ICTs, including, for example, regulations governing personal data protection and cross-border data transfer.[65]

Analysis

17. Recommendation (e) specifies that "in ensuring the secure use of ICTs", States should respect Human Rights Council

---

[62] See, for example, *The Global Principles on National Security and the Right to Information (Tshwane Principles)*, 12 June 2013; and *The International Principles on the Application of Human Rights to Communications Surveillance*, May 2014. For other initiatives, see 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 11 May 2016, A/HRC/32/38, para. 14.

[63] World Bank, *World Development Report 2016: Digital Dividends* (World Bank, 2016); and Global Commission on Internet Governance, *One Internet* (Centre for International Governance Innovation and The Royal Institute for International Affairs, 2016).

[64] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), Chapter 6.

[65] For a detailed overview of the various regulations governing these areas, see generally, Kriangsak Kittichaisaree, op. cit., pages 57-83.

resolutions 20/8 and 26/13, as well as General Assembly resolutions 68/167 and 69/166, so as "to guarantee full respect for human rights".

18. The resolutions referred to in the recommendation make clear that "the same rights that people have offline must also be protected online".[66] This approach has been described as a "normative equivalence paradigm" which equates respect and protection of offline rights with respect and protection of online rights.[67] According to this approach, "the digital, global and technologically innovative environment in which on-line rights operate represent a challenging (yet, at times, also promising) context for the interpretation and application of off-line rights, which requires the development of new policies, but do not necessarily require a re-evaluation of the contents of the rights themselves".[68]

19. The resolutions also refer to a number of specific practices—including State surveillance of communications,[69] combating advocacy of hatred,[70] and ensuring access to the Internet[71]—that raise particular human rights concerns in the cyber context. Additionally, the resolutions refer in general terms to ensuring respect for and the protection of the right to privacy and the right to freedom of expression online.[72] These provisions reflect an "institutional equivalence paradigm", which equates the role of States concerning offline rights

---

[66] A/HRC/20/8, para. 1; A/HRC/26/13, para. 1; A/RES/68/167, para. 3; and A/RES/69/166, para. 3. See similarly, Michael N. Schmitt (edop. cit., Rule 35 ("Individuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy").

[67] Y. Shany, 'Contribution to Open Consultation on UN GGE 2015 Norm Proposals' (2018), at 1, accessible online at the following link: http://csrcl.huji.ac.il/sites/default/files/csrcl/files/contribution_un_gge_norm_proposals-_dd.pdf (last accessed 26 March 2018).

[68] Ibid., at 2.

[69] A/RES/68/167, para. 4(d); and A/RES/69/166, para. 4(d)-(e).

[70] A/HRC/26/13, para. 6.

[71] A/HRC/20/8, para. 3; A/HRC/26/13, para. 3, 4 and 7.

[72] A/RES/68/167, para. 1 and 4(a)-(b); A/RES/69/166 (2014), para. 1 and 4(a)-(b); A/HRC/20/8, para. 1; A/HRC/26/13, para. 1.

with their role concerning online rights.[73] Importantly, as one commentator has observed, "[t]he role of private actors is treated in these resolutions to a limited degree only: they are stakeholders with which governments should engage, and they incur their own form of corporate social responsibility".[74]

20. At the outset, it is important to note that the adequacy of the normative and institutional equivalency paradigms is not self-evident. According to Yuval Shany, for example, cyberspace creates "new needs and interests, as well as new risks, which are not fully captured by existing paradigms".[75] Specifically, Shany points to:[76] new security risks that arise from the breadth and speed in which online data, hardware and software spreads and which underpin claims for a new right cyber security; new risks of manipulation of public opinion and thought control that arise from the spread of data combined with the sorting effects of algorithms and which may merit a different approach to speech regulation online; and the limited capacity of States to exercise a meaningful degree of regulatory control over the cyber domain due to the deterritorialized and decentralized attributes of cyberspace, characteristics that merit greater involvement and concern for the responsibilities of non-State actors.

21. While embracing a normative and institutional equivalence approach, the human rights recommendation leaves open precisely *how*, in ensuring the secure use of ICTs, States should guarantee full respect for human rights in practice.

22. Reflecting on this question, it is important to recognise at the outset that both customary and conventional international human rights law apply to cyber-related activities.[77] In this regard, it is also crucial to consider that the field of international

---

[73] Y. Shany, 'Contribution to Open Consultation on UN GGE 2015 Norm Proposals' (2018), at 2, accessible online at the following link: http://csrcl.huji.ac.il/sites/default/files/csrcl/files/contribution_un_gge_norm_proposals-_dd.pdf (last accessed 26 March 2018).

[74] Ibid.

[75] Ibid.

[76] Ibid., at 2-3.

[77] Michael N. Schmitt (ed.), *op. cit.*, at 179.

human rights law is particularly "thick with treaties",[78] many of which are widely ratified and equipped with treaty bodies or regional commissions and courts that evaluate state reports, deliver authoritative interpretations of the law, and/or determine individual complaints. As such, examining the human rights treaties to which States are party is the typical starting point for identifying how to guarantee full respect for human rights whilst ensuring the secure use of ICTs.

23. There are several challenges in relying on customary and conventional sources of international human rights law with respect to cyber-related activities. As the International Group of Experts that conducted the *Tallinn Manual 2.0* process have observed:[79]

> [I]t is often unclear as to whether certain human rights reflected in treaty law have crystallised as rules of customary law. Moreover, aspects of international human rights treaty law are subject to variance when States and regional bodies interpret them vis-à-vis cyber activities.

24. The purpose of this Commentary, however, is not to provide a restatement of existing customary or conventional human rights law. Rather, taking the framework of international human rights law—and its interpretation by, inter alia, treaty bodies, courts, experts, civil society groups, and scholars—as a reference point, this Commentary seeks to provide general guidance to States on how best to implement the voluntary and non-binding human rights norm proposed in the GGE 2015 Report.

25. As noted within the GGE 2015 Report, 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".[80] In line with this understanding of norms, this Commentary seeks to identify appropriate standards for responsible State

---

[78] Dinah. PoKempner, *Squinting Through the Pinhole: A Dim View of Human Rights from Tallinn 2.0* (95 *Texas Law Review,* 2017), page 1603.

[79] Michael N. Schmitt (ed.), *op. cit., page* 179.

[80] A/70/174, para. 10.

behaviour for guaranteeing full respect for human rights when ensuring the secure use of ICTs. For this purpose, this section is structured into six parts: (a) scope of application of the international human rights referenced within the human rights norm; (b) surveillance; (c) data protection; (d) encryption and anonymity; (e) access to content online; and (f) access to Internet infrastructure.

A. Scope of application

26. The first issue that requires clarification is the scope of application of the international human rights referenced within the human rights recommendation. For this purpose, it is necessary to examine the scope of application of international human rights law.

27. International human rights law has been characterised as "a system of norms and institutions that channels universal norms through the apparatus of the state system".[81] Over time, this conceptual structure has been put under strain by three developments:[82] first, the exercise of power and control over individuals by *non-State actors*; second, the *extraterritorial* exercise of State authority; and third, the *extraterritorial* exercise of non-State authority. The emergence of cyberspace in recent decades has served to exacerbate these developments.

28. Turning first to the increasing influence of non-State actors, the United Nations Special Rapporteur on Freedom of Expression has recently explained that "[t]he private sector's role in the digital age appears pervasive and ever-growing, a driving force behind the greatest expansion of access to

---

[81] Yuval Shany, *Cyberspace: The Final Frontier of Extra-Territoriality in Human Rights Law* (*HUJI Cyber Security Research Center Blog*, September 2017).

[82] Ibid. See similarly, N. Tsagourias, *Legal Status of Cyberspace*, in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2015) pages 21-22 (observing "the deterritorialisation of sovereignty"); and David P. Fidler, *Cyberspace and Human Rights*, in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2015) pages 98-99.

information in history".[83] In particular, the private sector invests in, maintains and in many cases owns vast social media forums, the infrastructure for mobile technology, the tools used by law enforcement and intelligence for surveillance and data-processing, and the devices or services on which most personal data is stored.

29. The conceptual framework of international human rights law has responded to the increasing influence of non-State actors in two ways: First, States must not only *respect* human rights, but also *protect* them.[84] The obligation to respect entails a negative obligation to refrain from violating rights. The obligation to *protect* entails a positive obligation to ensure enjoyment of those rights, which may require a State to take steps to protect individuals from the actions of non-State actors. Second, although international human rights law has traditionally been State-centric, various routes have been developed to extend the application of human rights norms to non-State actors.[85] In particular, domestic legislation may require human rights due diligence from certain non-State actors, expressly or implicitly drawing on the content of regional and international human rights instruments. In addition, the United Nations Guiding Principles on Business and Human Rights have elaborated the responsibility to respect human rights as a global standard of expected conduct for all business enterprises wherever they operate.[86]

---

[83] A/HRC/32/38, para. 1.

[84] See, for example, A/HRC/32/38, para. 8; Human Rights Committee, 'General Comment 31—The Nature of the General Legal Obligations Imposed on States Parties to the Covenant', 29 March 2004, CCPR/C/21/Rev.1/Add.13, para. 6; and Michael N. Schmitt (ed.), *op. cit.,* Rule 36.

[85] See generally, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 11 May 2016, U.N.Doc. A/HRC/32/38, at paras 9-14.

[86] See generally, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, in *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Entities*, A/HRC/17/31, 21 March 2011.

30. Beyond enhancing the influence of non-State actors, the emergence of cyberspace has also provided heightened opportunities for the *extraterritorial* exercise of *State* authority. For present purposes, extraterritoriality encompasses two scenarios: first, the exercise of State authority beyond its territorial borders; and second, the exercise of State authority within its territorial borders but with extraterritorial effects upon individuals across the globe. Although the jurisdictional competence of a State is primarily based on the principle of territoriality,[87] all major international courts and human rights bodies—including the International Court of Justice, the United Nations Human Rights Committee, the Inter-American Commission on Human Rights, and the European Court of Human Rights—agree that in some circumstances human rights obligations apply extraterritorially.[88] In other words, it is well-

---

[87] See, for example, Article 2(1), International Covenant on Civil and Political Rights ("Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant") (emphasis added); Article 1, European Convention on Human Rights ("High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention"); and M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), at 183 (referring to customary international law).

[88] See generally, N. Lubell, *Extraterritorial Use of Force Against Non-State Actors* (OUP, 2010), at 193-207. In the cyber surveillance context, see Human Rights Committee, 'Concluding observations on the fourth periodic report of the United States of America', U.N. Doc. CCPR/C/USA/CO/4, 23 April 2014, at para. 22 ("measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessary, *regardless of the nationality or location of the individuals whose communications are under direct surveillance*") (emphasis added). Some States remain opposed to the extraterritorial application of human rights. Most prominently, the United States has long denied that it has obligations to respect and ensure human rights beyond its territorial borders. See, in this regard, Human Rights Committee, 'Summary Record of the 1405th Meeting', U.N.Doc. CCPR/C/SR/1405, 24 April 1995, at para. 20 ("The [ICCPR] was not regarded as having extraterritorial application […] Article 2 of the Covenant expressly stated that each State party undertook to respect and ensure the rights recognized 'to all individuals within its territory and subject to its jurisdiction'. That dual requirement

established that States are bound by international human rights law with respect to individuals who are not physically located within their territorial borders, but who nonetheless fall within their jurisdiction.[89]

31. Reviewing the conditions and circumstances pursuant to which international human rights law applies extraterritorially, a useful starting point is to note that, whether pursuant to customary international law or relevant treaty law, it is generally accepted that international human rights law applies beyond a State's territory to any individual within the "power or effective control" of the State.[90] Under this threshold, two types of extraterritorial jurisdiction may be distinguished.

32. First, pursuant to the *spatial* model, human rights law applies to individuals located in a territory under a State's

---

restricted the scope of the Covenant to persons under United States jurisdiction and within United States territory").

[89] In the context of human rights treaties, Lubell defines the term "jurisdiction" as "the responsibility of states towards an individual". N. Lubell, *Extraterritorial Use of Force Against Non-State Actors* (OUP, 2010), at 209. See also, E. Watt, 'The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance', in H. Röigas et al. (eds.), *2017 9th International Conference on Cyber Conflict: Defending the Core* (NATO CCD COE Publications, 2017) 93, at 100.

[90] See, for example, Human Rights Committee, 'General Comment 31—The Nature of the General Legal Obligations Imposed on States Parties to the Covenant', 29 March 2004, U.N.Doc. CCPR/C/21/Rev1/Add.13, at para. 10 (setting out the "power or effective control" extraterritoriality threshold with respect to the ICCPR); *Al-Skeini v. United Kingdom*, Application No. 55721/07, European Court of Human Rights, Judgment, 2011, at paras 133-140 (setting out the "State agent authority and control" and "effective control over an area" extraterritoriality thresholds with respect to the ECHR); *Alexandre v. Cuba*, Case 11.589, Inter-American Commission on Human Rights, IACHR Report No. 109/99, 1999, at para. 37 ("the inquiry [with respect to the IACHR] turns not on the presumed victim's nationality, or presence within a particular geographical area, but on whether under specific circumstances, the State observed the rights of a person subject to its authority and control"); and M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), at 184 (referring to the "power or effective control" threshold under customary international law).

effective control.[91] In this scenario, States must satisfy both their negative obligation to respect and their positive obligation to protect the human rights of individuals within territory under their control.[92]

33. Second, pursuant to the *personal* model, human rights law applies to individuals under a State's power or effective control.[93] In terms of the types of obligations that are applicable in this scenario, it is well-established that States must fulfill their negative obligation to respect the human rights of individuals under their control. However, it may be that only

---

[91] See, for example, Human Rights Committee, 63rd Session, *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant: Concluding Observations*: Israel, 15-28 July 1998, CCPR/C/79/Add.93, para. 10 ("[T]he Covenant must be held applicable to the occupied territories and those areas […] where Israel exercise effective control."); *Al-Skeini v. United Kingdom*, Application No. 55721/07, European Court of Human Rights, Judgment, 2011, paras 138-140 (setting out the "effective control over an area" extraterritoriality threshold with respect to the ECHR); and M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), at 184 (referring to the spatial model under customary international law).

[92] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', 56 *Harvard International Law Journal* (2015) 81, at 123. See also, M Michael N. Schmitt (ed.), *op. cit., pages* 196-198 (outlining the division of opinion between the International Group of Experts on "the precise territorial circumstances in which a State has an obligation to protect a particular individual's human rights from interference by third parties").

[93] See, for example, Human Rights Committee, *General Comment 31—The Nature of the General Legal Obligations Imposed on States Parties to the Covenant*, 29 March 2004, CCPR/C/21/Rev1/Add.13, para. 10 ("a State Party [to the ICCPR] must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party […] regardless of the circumstances in which such power or effective control was obtained"); *Al-Skeini v. United Kingdom*, Application No. 55721/07, European Court of Human Rights, Judgment, 2011, paras 133-136 (setting out the "State agent authority and control" extraterritoriality threshold with respect to the ECHR); Michael N. Schmitt (ed.), *op. cit., page* 184 (referring to the personal model under customary international law).

those specific rights relevant to the situation will be engaged.[94] Moreover, it remains a matter of contestation whether States must also fulfill their positive obligation to protect the human rights of individuals under their control.[95]

34. In addition, it is important to note that although control pursuant to the personal model has traditionally been understood to mean physical control over an individual, recent international human rights caselaw and reports suggest that this threshold is becoming more permissive.[96]

(a) In its report on the right to privacy in the digital age, the Office of the United Nations High Commissioner for Human Rights stated that human rights obligations of States are engaged by digital surveillance in the following circumstances:[97]

---

[94] *Al-Skeini v. United Kingdom*, Application No. 55721/07, European Court of Human Rights, Judgment, 2011, para. 137; and M.N. Schmitt (ed.), Michael N. Schmitt (ed.), *op. cit., page* 184.

[95] Compare, for example, Human Rights Committee, *General Comment 31—The Nature of the General Legal Obligations Imposed on States Parties to the Covenant*, 29 March 2004, CCPR/C/21/Rev1/Add.13, para. 10 (asserting that a State must both "respect *and ensure*" the rights of individuals within its power or effective control); and Michael N. Schmitt (ed.), *op. cit., pages* 197-198 (confining a State's positive obligation to protect to individuals "within their territories or territories under their exclusive governmental control").

[96] See similarly, Eliza Watt, *The Right to Privacy and the Future of Mass Surveillance* (21 *The International Journal of Human Rights,* 2017), page 778; and Vivian Ng and Daragh Murray, *Extraterritorial Human Rights Obligations in the Context of State Surveillance Activities?* (*HRC Essex Blog*, 2 August 2016). See, however, *Human Rights Watch Inc & Others v. Secretary of State for Foreign and Commonwealth Affairs & Others*, UK Investigatory Powers Tribunal, [2016] UKIPTrib 15_11-CH, 16 May 2016, at para. 60 (concluding that "a contracting state owes no obligation under Article 8 [ECHR] to persons both of whom are situated outside its territory in respect of electronic communications between them which pass through that state").

[97] 'Report of the Office of the UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age', 30 June 2014, U.N.Doc. A/HRC/27/37, at para. 34 (emphasis added). See similarly, 'Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', 23 September 2014, U.N.Doc. A/69/397, at para. 41; and 'Advisory Opinion OC-23/17: Environment and Human Rights', Inter-American

> [D]igital surveillance […] may engage a State's human rights obligations if that surveillance involves *the State's exercise of power or effective control in relation to digital communications infrastructure*, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where *the State exercises regulatory jurisdiction over a third party that physically controls the data*, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty.

According to this passage, the human rights obligations of a State may be engaged in relation to any person—irrespective of their nationality or physical location—whenever a State exercises effective control over the communications infrastructure through which privacy rights are interfered with.[98]

(b) In addition, in *Jaloud v. The Netherlands*, the European Court of Human Rights found that the Netherlands exercised jurisdiction over an individual passing through a checkpoint manned by Dutch agents on the basis that they

---

Court of Human Rights, 15 November 2017, at para. 104(h) ("As regards transboundary harms, a person is under the jurisdiction of the State of origin if there is a causal relationship between the event that occurred in its territory and the affectation of the human rights of persons outside its territory. The exercise of jurisdiction arises when the State of origin exercises *effective control over the activities carried out that caused the harm* and consequent violation of human rights") (author's own translation, emphasis added).

[98] For critique of this approach, see M. Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', 56 *Harvard International Law Journal* (2015) 81, at 145 (arguing that "the concept of power and control over communications infrastructure does not fit well with the existing case law […] [n]or does it seem adequate for those types of surveillance that require no control over the infrastructure at all.").

exercised authority and control over the individual's right to life at that moment.[99] For several commentators, this case indicates that the European Court of Human Rights is "moving towards an understanding that exercising authority and control *over an individual's rights* gives rise to extraterritorial jurisdiction and obligations in relation to those affected rights".[100]

35. Finally, it should also be noted that some scholars have suggested that a preferable approach to the question of the extraterritorial application of international human rights law would be to distinguish between negative and positive obligations.[101] According to this approach, the negative obligation to respect human rights would be territorially unlimited and not subject to any jurisdictional threshold, while the positive obligation to secure or ensure human rights would be predicated on a State having effective control over a territory. The rationale for this approach is that in general a State will need control over a territory to comply with its positive obligations, whereas it will always have the capacity to comply

---

[99] *Jaloud v. The Netherlands*, Application No. 47708/08, European Court of Human Rights, Judgment, 20 November 2014, para. 152.

[100] Vivian Ng and Daragh Murray, op. cit. (emphasis added). See similarly, Eliza Watt, *The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance*, in Henri Rõigas et al. (eds.), *9th International Conference on Cyber Conflict: Defending the Core* (NATO CCD COE Publications, 2017), page 102. A majority of the International Group of Experts within the *Tallinn Manual 2.0* process, however, took the view that "physical control over territory or the individual is required before human rights law obligations are triggered". Only a few of the Experts took the position that "so long as the exercise or enjoyment of a human right in question by the individual is concerned is within the power or effective control of a State, that State has power or effective control over the individual with respect to the right concerned". See Michael N. Schmitt (ed.), *op. cit., page* 185.

[101] See, in particular, Marko Milanovic, op. cit., pages 118-119; and Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism* (Fordham Law Review, 2014) pages 2148-2150. See also, N. Lubell, *Extraterritorial Use of Force Against Non-State Actors* (OUP, 2010), at 227-231.

with its negative obligations.[102] To date, however, this approach has not been adopted by any human rights courts or bodies.[103]

36. A final development that has been exacerbated by the emergence of cyberspace is the exercise of *extraterritorial* authority by *non-State* actors. This development gives particular significance to the question of the scope of extraterritorial human rights obligations owed by States—in particular the extent to which States are required to take "the steps necessary to prevent human rights violations abroad by corporations domiciled in their territory and/or jurisdiction (whether they were incorporated under their laws, or had their statutory seat, central administration or principal place of business on the national territory), without infringing the sovereignty or diminishing the obligations of the host States".[104]

37. The approach of the United Nations Human Rights Committee in these scenarios has been to require States to "ensure that all activities taking place in whole or in part within their territory and in other areas subject to their jurisdiction, but having a [direct], significant and foreseeable impact" on rights outside their territory, including activities taken by corporate entities, are consistent with the ICCPR, "taking due account of related international standards of corporate social responsibility".[105]

---

[102] Marko Milanovic, op. cit., page 119. See also, N. Lubell, *Extraterritorial Use of Force Against Non-State Actors* (OUP, 2010), at 230 (arguing for "a contextual approach to obligations" whereby "the extent to which contracting parties must secure the rights and freedoms of individuals outside their borders is proportionate to the extent of their control over these individuals").

[103] Marko Milanovic, op. cit., page 129 (emphasising that his approach is "what the Court *should* do") (emphasis in original).

[104] United Nations Committee on Economic, Social and Cultural Rights, *General Comment No. 24 (2017) on State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities*, 10 August 2017, E/C.12/GC/24, para. 26.

[105] United Nations Human Rights Committee, *General Comment No. 36 on Article 6 on the International Covenant on Civil and Political Rights, on the Right to Life*, Revised Draft Prepared by the Rapporteur, para. 26. See also, United Nations Human Rights Committee, *Concluding Observations*: Canada (2015), para. 6.

38. In its recent General Comment No. 24, the Committee on Economic, Social and Cultural Rights confirmed that in these types of scenarios States are required "to take reasonable measures that could have prevented the occurrence" of human rights violations that occur outside their territories due to the activities of business entities over which they can exercise control.[106] The responsibility of States can be engaged in such circumstances "even if other causes have also contributed to the occurrence of the violation, and even if the State had not foreseen that a violation would occur, provided such a violation was reasonably foreseeable".[107] In addition, the Committee has noted that States "should also require corporations to deploy their best efforts to ensure that entities whose conduct those corporations may influence, such as subsidiaries […] or business partners […] respect Covenant rights".[108] Finally, the Committee confirmed that States must put in place "[a]ppropriate monitoring and accountability procedures […] to ensure effective prevention and enforcement".[109]

39. Reflecting on these standards, Yuval Shany has argued that caution is required in terms of how States should comply with their positive obligations to protect human rights in these scenarios.[110] In particular, Shany argues that it is important to ensure that international human rights law does not require States "to *renationalize* segments of cyberspace and to fragment it to overlapping territorial zones of influence and regulation", in such a way that would cut against the universality of cyberspace.[111] Rather, international human rights law in this context should be limited to requiring States to encourage

---

[106] United Nations Committee on Economic, Social and Cultural Rights, *General Comment No. 24 (2017) on State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activiti*es, 10 August 2017, E/C.12/GC/24, para. 32.

[107] Ibid.

[108] Ibid., para. 33.

[109] Ibid., para. 33.

[110] Yuval Shany, *Cyberspace: The Final Frontier of Extra-Territoriality in Human Rights Law* (HUJI Cyber Security Research Center Blog, September 2017).

[111] Ibid. (emphasis in original).

private companies over which they can exercise control "to adopt generally acceptable standards of corporate responsibility […], [as well as] support and oversee self-regulation, private ordering and coding by the industry and support hybrid norms and institutions that apply globally".[112]

B. Surveillance

40. For the purposes of this Commentary, "surveillance" will be understood in broad terms as an umbrella concept encompassing a range of practices that are conducted for the purpose of gathering intelligence, including "the monitoring intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future".[113]

41. The emergence of cyberspace has changed not only how surveillance can be carried, but also what can be monitored.[114] As the United Nations Special Rapporteur on Counter-Terrorism has observed:[115]

---

[112] Ibid.

[113] International Principles on the Application of Human Rights to Communications Surveillance (2013), at 4. See similarly, A/HRC/23/40, para. 6 (defining "communications surveillance" as "the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communication networks"). On the varied terminology related to "surveillance measures in the digital age", see generally, European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume II: Field Perspectives and Legal Update* (Publications Office of the European Union, 2017), pages 29-32; and European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume I: Member States' Legal Frameworks* (Publications Office of the European Union, 2015), pages 13-27.

[114] A/HRC/23/40, para. 15.

[115] A/69/397, para. 8. For an overview of the different modalities of communications surveillance, see generally, A/HRC/23/40, para. 33-49.

> By placing taps on fibre-optic cables through which the majority of digital communications travel, relevant States have [...] been able to conduct mass surveillance of communications content and metadata, providing intelligence and law enforcement agencies with the opportunity to monitor and record not only their own citizens' communications, but also the communications of individuals located in other States.

42. In addition, according to the Berkman Center for Internet & Society, the emergence of the Internet of Things, with audio and video sensors attached to a wide range of devices, "will open up numerous avenues for government actors to demand access to real-time and recorded communications".[116]

43. States are required to ensure that the design and implementation of surveillance practices conform with the requirements of international human rights law, in particular the right to privacy as defined in customary international law and—if the State is party to a relevant treaty—conventional international law.[117] In this regard, bearing in mind that privacy serves as a basis for other rights such as freedom of expression, association, and movement, it is also important to emphasise at the outset that surveillance regimes may have "a profound chilling effect on other fundamental rights".[118]

44. In determining conformity with the right to privacy, human rights courts and bodies have generally adopted a four-part test:[119] (a) Has there been an interference with an individual's

---

[116] Berkman Center for Internet & Society, *Don't Panic: Making Progress on the 'Going Dark' Debate* (1 February 2016), page 13. See similarly, World Bank, *World Development Report 2016: Digital Dividends* (World Bank, 2016), page 225.

[117] With respect to custom, see Michael N. Schmitt (ed.), *op. cit., page* 189 ("the right [to privacy] is of a customary law character"). In terms of treaty law, see, for example, Article 17, ICCPR; Article 8, ECHR; and Article 11, ACHR.

[118] A/HRC/13/37, para. 33.

[119] See, for example, A/69/397, para. 28-30; A/HRC/27/37, para. 15-41; A/HRC/23/40, para. 15-30; A/HRC/13/37, para. 11-19; European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume*

privacy? (b) If so, was the interference in accordance with the law? (c) If so, did the interference pursue a legitimate aim? (d) If so, was the interference necessary and proportionate to that aim?

45. In practice, the analysis of these questions tends to vary to some extent depending on the applicable legal regime.[120] For the purpose of interpreting the human rights norm proposed in the GGE 2015 Report, it is suggested that States should draw particular guidance from the findings of the United Nations Human Rights Committee,[121] the European Court of Human Rights, and the Court of Justice of the European Union, as well as the analysis and recommendations of various United Nations Special Rapporteurs, the Office of the United Nations High Commissioner for Human Rights, civil society groups and scholars.

46. Privacy has been defined in general terms as "the presumption that individuals should have an area of personal autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals", as well as "the right of individuals to know who holds information about them and how that information is used".[122]

II: Field Perspectives and Legal Update (Publications Office of the European Union, 2017), page 33; and Marko Milanovic, op. cit., page 133.

[120] Peter Margulies, op. cit., pages 4-5 ("international law on privacy must recognize that states have a range of conceptions of privacy, as well as a broad spectrum of legal and political institutions that intersect with privacy guarantees"). See also, A/HRC/31/64, para. 21 ("The existence and usefulness of this legal framework is however seriously handicapped by the lack of a universally agreed and accepted definition of privacy").

[121] For detailed references to the work of the UN Human Rights Committee concerning surveillance practices of States, see generally Y. Shany, 'Contribution to Open Consultation on UN GGE 2015 Norm Proposals' (2018), accessible online at the following link: http://csrcl.huji.ac.il/sites/default/files/csrcl/files/contribution_un_gge_norm_proposals-_dd.pdf (last accessed 26 March 2018).

[122] A/69/397, para. 28. See similarly, A/HRC/23/40, para. 22; and A/HRC/13/37, para. 11. For useful overviews of recent jurisprudence on

47. The United Nations Human Rights Committee has confirmed that the right to privacy requires that "the integrity and confidentiality of correspondence should be guaranteed de jure and de facto".[123] This right to private correspondence gives rise to a comprehensive obligation of the State "to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties".[124]

48. The United Nations Human Rights Committee has also indicated that "[t]he gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law".[125]

49. In addition to the content of communications, the interception or collection of data about a communication—often referred to as "metadata"—may also constitute an interference with privacy.[126] According to the Court of Justice of the European Union, metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[127] With this in mind,

---

the meaning of "privacy", see generally. Eliza Watt, 'op. cit., at 778-779; and Marko Milanovic, op. cit., at 134.

123 Human Rights Committee, *General Comment No. 16—Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation),* 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I), para. 8.

124 A/HRC/23/40, para. 24.

125 Human Rights Committee, 'General Comment No. 16—Article 17, op. cit., para. 10. See also, A/HRC/13/37, para. 12 (noting that "data protection is also emerging as a distinct human or fundamental right"); and A/HRC/17/27, para. 58.

126 See, for example, *Copland v. United Kingdom*, Application No. 62617/00, European Court of Human Rights, Judgment, 3 April 2007, para. 41; *Malone v. United Kingdom*, Application No. 8691/79, European Court of Human Rights, Judgment, 26 April 1985, at pars 83-84; and International Principles on the Application of Human Rights to Communications Surveillance (2013), at 4-5.

127 *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union, Judgment, 8 April 2014, paras 26-27 and 37. See similarly, 'Report of the Office of the United Nations High Commissioner for Human Rights: The Right

the Office of the United Nations High Commissioner for Human Rights has concluded that "any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used".[128]

50. The European Court of Human Rights has also confirmed that "the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference".[129]

51. Finally, the European Court of Human Rights has confirmed that even "the mere existence of legislation which allows a system for the secret monitoring of communications […] amounts in itself to an interference" with the right to privacy.[130]

52. In order for an interference with an individual's right to privacy to be permissible, it must be conducted in accordance

---

to Privacy in the Digital Age', 30 June 2014, A/HRC/27/37, para. 19; 'Report of the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', 23 September 2014, A/69/397, paras 53-55; and A/RES/69/166 (2014), A/RES/69/166, 18 December 2014, at Preamble ("*Noting* that while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and given an insight into an individual's behaviour, social relationships, private preferences and identity'). For an overview of recent jurisprudence recognizing the privacy concerns raised by the interception or collection of metadata, see generally C. Nyst and T. Falchetta, 'The Right to Privacy in the Digital Age', 9 *Journal of Human Rights Practice* (2017) 104, at 110-112.

128 A/HRC/27/37, para. 20.

129 *Weber and Saravia v. Germany*, Application No. 54934/00, European Court of Human Rights, Decision, 29 June 2006, para. 79.

130 *Weber and Saravia v. Germany*, Application No. 54934/00, European Court of Human Rights, Decision, 29 June 2006, para. 78. See similarly, 'Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age', 30 June 2014, A/HRC/27/37, para. 20 ("The very existence of a mass surveillance programme thus creates an interference with privacy").

with the law.[131] This condition requires not only that surveillance have a basis in a State's domestic law, but also that the law possess certain qualities.[132]

53. First, the law must be accessible to the public, formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly, and not confer unfettered discretion.[133] In *Zakharov v. Russia*, the European Court

---

[131] See, for example, Article 17 ICCPR ("unlawful"); Article 8(2) ECHR ("in accordance with the law"); Michael N. Schmitt (ed.), op. cit., pages 206-207 (elaborating this condition under customary international law); and International Principles on the Application of Human Rights to Communications Surveillance (2013), at 7 ("Legality").

[132] See, for example, Human Rights Committee, 'General Comment No. 16—Article 17, op. cit., para. 3 ("The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."); Human Rights Committee, 'Concluding observations on the sixth periodic report of Italy', U.N.Doc. CCPR/C/IT/CO/6, 1 May 2017, at para. 36 ("The Committee is concerned about reports that intelligence agencies are intercepting personal communications and employing hacking techniques without explicit statutory authorization or clearly defined safeguards from abuse"); and *Roman Zakharov v. Russia*, Application No. 47143/06, European Court of Human Rights, Judgment, 4 December 2015, para. 228 (referring to "quality requirements"). See generally in the surveillance context, Marko Milanovic, *op. cit.*, at 134-136; and Eliza Watt, *op. cit.*, at 780-781.

[133] Human Rights Committee, 'General Comment No. 34—Freedom of Opinion and Expression', ICCPR 12 September 2011, Document CCPR/C/GC/34, para. 25. See similarly, Human Rights Committee, 'Concluding observations on the fourth periodic report of the United States of America', U.N.Doc. CCPR/C/USA/CO/4, 23 April 2014 ("The Committee is concerned that, until recently, judicial interpretations of FISA and rulings of the Foreign Intelligence Surveillance Court (FISC) had largely been kept secret, thus not allowing affected persons to know the law with sufficient precision"); Human Rights Committee, 'Concluding observations on the fourth periodic report of Switzerland', U.N.Doc. CCPR/C/CHE/CO/4, 22 August 2017, at para. 46 ("the Committee is concerned that this law grants very intrusive surveillance powers to the Confederation's intelligence services on the basis of insufficiently defined objectives such as the national interest, referred to in article 3. It is also concerned that the time period for which data may be retained is not specified (art. 17)"); *Roman Zakharov v. Russia*, Application No. 47143/06, European Court of Human Rights, Judgment,

of Human Rights explained that the domestic law must be sufficiently clear to give individuals an adequate indication of the circumstances in which and the conditions on which public authorities are empowered to resort to surveillance measures, as well as indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[134] The Court also set out the following minimum safeguards that should be set out in law to avoid abuses of power with respect to secret measures of surveillance:[135]

> [T]he nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed.

54. The legality requirement also requires effective procedural safeguards, including effective, adequately resourced institutional arrangements.[136] According to the United Nations

---

4 December 2015, para. 228 (confirming that the law "must be accessible to the person concerned and foreseeable as to its effects"); A/HRC/27/37, paras 28-30; A/69/397, paras 35-40; International Principles on the Application of Human Rights to Communications Surveillance (2013), at 10 ("Transparency").

[134] *Roman Zakharov v. Russia*, Application No. 47143/06, European Court of Human Rights, Judgment, 4 December 2015, paras 229-230. See similarly, 'Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age', 30 June 2014, A/HRC/27/37, para. 28.

[135] *Roman Zakharov v. Russia*, Application No. 47143/06, European Court of Human Rights, Judgment, 4 December 2015, para. 231. See similarly, 'Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age', 30 June 2014, A/HRC/27/37, para. 28.

[136] A/HRC/27/37, para. 37; A/69/397, para. 45-50; and International Principles on the Application of Human Rights to Communications Surveillance (2013), at 9-10 ("Competent Judicial Authority", "Due

Special Rapporteur on Counter-Terrorism, although these safeguards may take a variety of forms, they generally include "independent prior authorization and/or subsequent independent review".[137] In this regard, the Office of the United Nations High Commissioner for Human Rights, has emphasised that "the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law".[138]

55. States are also required to ensure that the victims of privacy violations have access to an effective remedy.[139] According to the Office of the United Nations High Commissioner for Human Rights, effective remedies typically share the following characteristics:[140] they must be "known and accessible to anyone with an arguable claim that their rights have been violated"; they will involve "prompt, thorough and impartial investigation of alleged violations" provided through the provision of an independent oversight body; they must be

---

Process", and "Public Oversight"). See also, Human Rights Committee, 'Concluding observations on the fifth periodic report of France', U.N.Doc. CCPR/C/FRA/CO/5, 17 August 2015, at para. 12 ("The Committee is particularly concerned about the fact that the law on intelligence adopted on 24 June 2015 (submitted to the Constitutional Court) gives the intelligence agencies excessively broad, highly intrusive surveillance powers on the basis of broad and insufficiently defined objectives, without the prior authorization of a judge and without an adequate and independent oversight mechanism (art. 17)."); and Human Rights Committee, 'Concluding observations on the sixth periodic report of Italy', U.N.Doc. CCPR/C/ITA/CO/6, 1 May 2017, at para. 37 ("The State party should review the regime regulating the interception of personal communications, the hacking of digital devices and the retention of communications data with a view to ensuring: […] (b) that robust, independent oversight systems are in place regarding surveillance, interception and hacking, including by ensuring that the judiciary is involved in the authorization of such measures, in all cases, and by affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were placed under surveillance or that their data was hacked").

137 A/69/397, para. 45.

138 A/HRC/27/37, para. 37.

139 See, for example, Article 2(3) ICCPR; and Article 13 ECHR.

140 A/HRC/27/37, paras 40-41.

"capable of ending ongoing violations"; and "where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required". The United Nations Special Rapporteur on Counter-Terrorism has also noted that in order to render the right to privacy effective, "domestic law must provide an independent mechanism capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process guarantees, which has power to grant a binding remedy (including, where appropriate, an order for the cessation of surveillance or the destruction of the product)".[141] Finally, in *Zakharov v. Russia*, the European Court of Human Rights has clarified that information about interception of communications and available remedies should be provided to the persons concerned "[a]s soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure".[142]

56. The United Nations Special Rapporteur on Counter-Terrorism has observed that extraterritorial surveillance operations pose unique challenges to the legality requirement.[143] In particular, domestic legislation often affords less protection to external (international) communications compared to purely domestic communications, as well as permits asymmetrical protection for nationals and non-nationals. According to the Special Rapporteur, "[e]ither form of differential treatment is incompatible with the principle of non-discrimination […] [and] States are legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction".[144]

---

[141] A/69/397, para. 49.

[142] *Roman Zakharov v. Russia*, Application No. 47143/06, European Court of Human Rights, Judgment, 4 December 2015, para. 287. See similarly, International Principles on the Application of Human Rights to Communications Surveillance (2013), at 9-10 ("User Notification").

[143] A/69/397, para. 42.

[144] A/69/397, para. 43. See similarly, Human Rights Committee, 'Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland', U.N.Doc. CCPR/C/GBR/CO/7, 17 August 2015 ("The Committee is concerned

57. International intelligence-sharing arrangements also raise particular legality concerns. The United Nations Special Rapporteur on Counter-Terrorism has observed that where an individual's communications are shared with foreign intelligence agencies without the protection of any publicly accessible legal framework or adequate safeguards, such practices "make the operation of the surveillance regime unforeseeable for those affected by it" and are therefore incompatible with the right to privacy.[145]

58. In addition to the legality requirement, States must also justify any interference with an individual's privacy on the basis of a legitimate aim.[146] Article 8 of the ECHR provides a list of legitimate aims, which include "national security, public safety

---

(a) that the Regulation of Investigatory Powers Act 2000, which makes a distinction between "internal" and "external" communications, provides for untargeted warrants for the interception of external private communications and communications data that are sent or received outside the United Kingdom without affording the same safeguards as apply to the interception of internal communications"); and Human Rights Committee, 'Concluding observations on the sixth periodic report of New Zealand', U.N.Doc. CCPR/C/NZL/CO/6, 28 April 2016, at para. 15 ("The Committee is further concerned about the limited judicial authorization process for the interception of communications of New Zealanders and the total absence of such authorization for the interception of communications of non-New Zealanders (art. 17)"). For an alternative view, see P. Margulies, op. cit., page 3 ("it is not arbitrary for a state to provide less extensive privacy rights to foreign nationals overseas than it provides to its own nationals").

145 A/69/397, para. 44. See similarly, Human Rights Committee, 'Concluding observations on the seventh periodic report of Sweden', U.N.Doc. CCPR/C/SWE/CO/7, 28 April 2016, at para. 37 ("It should ensure: (a) that all laws and policies regulating the intelligence-sharing of personal data are in full conformity with its obligations under the Covenant, in particular article 17, including the principles of legality, proportionality and necessity"); A/HRC/27/37, para. 30; and International Principles on the Application of Human Rights to Communications Surveillance (2013), at 11 ("Safeguards for International Cooperation").

146 See, for example, Michael N. Schmitt (ed.), *op. cit.,* pages 206-207 (noting that under customary international law "[l]imitations are lawful only if they serve a legitimate purpose"); International Principles on the Application of Human Rights to Communications Surveillance (2013), at 7 ("legitimate aim").

or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others".[147] According to the Office of the United Nations High Commissioner for Human Rights, "[s]urveillance on the grounds of national security or for the prevention of terrorism or other crime may be a 'legitimate aim'" for the purpose of Article 17 of the ICCPR.[148] The onus is on the State seeking to limit the right to show that the limitation is connected to the specified legitimate aim.[149]

59. Any interference with the right to privacy must also constitute a necessary and proportionate means to achieving the legitimate aim.[150] This condition requires: "a rational connection between the means employed and the aim sought to be achieved";[151] that the measure chosen be "the least intrusive instrument among those which might achieve the desired result";[152] "balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest";[153] and that "any limitation to the right to privacy […] not render the essence of the right meaningless and [...] be consistent with other human rights, including the prohibition of discrimination".[154] The onus is on the State to demonstrate that interference is both necessary and proportionate to the legitimate aim being addressed.[155]

---

147 Article 8(2) ECHR.

148 A/HRC/27/37, para. 24. See A/69/397, para. 33 ("the prevention, suppression, and investigation of acts of terrorism clearly amount to a legitimate aim").

149 A/HRC/27/37, para. 23.

150 See, for example, Article 17(1) ICCPR ("arbitrary"); Article 8(2) ECHR ("necessary in a democratic society"); and International Principles on the Application of Human Rights to Communications Surveillance (2013), at 7-8 ("necessity", "adequacy", and "proportionality").

151 A/69/397, para. 51.

152 Ibid.

153 Ibid.

154 A/HRC/27/37, para. 23.

155 Ibid., para. 25.

60. In its examination of necessity and proportionality, the European Court of Human Rights in *Zakharov v. Russia* provided additional guidance in the surveillance context. The entity competent to authorize the surveillance must be independent and "capable of verifying the existence of a reasonable suspicion against the person concerned, in particular whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security".[156] The interception authorisation "must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information".[157]

61. Based on the necessity and proportionality requirement, it has been suggested that States should avoid particular types of surveillance programmes. A range of reports and judicial findings have called into question the compatibility of mass surveillance programmes with the right to privacy. According to the United Nations Special Rapporteur on Counter-Terrorism, "the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy".[158] Similarly, the Office of the United Nations High Commissioner for Human Rights has concluded that "[m]ass or 'bulk surveillance programmes may […] be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime […] [because] it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened;

---

[156] *Roman Zakharov v. Russia*, Application No. 47143/06, European Court of Human Rights, Judgment, 4 December 2015, para. 260.

[157] *Roman Zakharov v. Russia*, Application No. 47143/06, European Court of Human Rights, Judgment, 4 December 2015, para. 264.

[158] A/69/397, paras 18 and 51-52.

namely, whether the measure is necessary and proportionate".[159] In *Schrems v. Data Protection Commissioner*, without making factual findings concerning the existence of mass surveillance programmes operated by the United States, the Court of Justice of the European Union found that "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life".[160]

62. The necessity and proportionality of systems of mandatory third-party data retention—where States require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access—have also been called into question.[161]

---

[159] A/HRC/27/37, para. 25. See also, Human Rights Committee, 'Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland', U.N.Doc. CCPR/C/GBR/CO/7, 17 August 2015 ("The Committee is concerned that the State party's current legal regime governing the interception of communications and communication data allows for mass interception of communications… The Committee is further concerned that the 2014 Data Retention Investigatory Powers Act provides for wide powers of retention of communication data and access to such data does not appear to be limited to the most serious crimes").

[160] *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, Court of Justice of the European Union, Judgment, 6 October 2015, para. 94 (citations omitted).

[161] See, for example, A/HRC/27/37, para. 26 ("appears neither necessary nor proportionate"); A/69/397, para. 53-55; Human Rights Committee, 'Concluding observations on the fourth periodic report of the United States of America', U.N.Doc. CCPR/C/USA/CO/4, 23 April 2014 ("Refrain from imposing mandatory retention of data by third parties"); *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union, Judgment, 8 April 2014; and *Watson and Others*, Joined Cases C-203/15 and C-698/15, Court of Justice of the European Union, Judgment, 21 December 2016. See also, International Principles on the Application of Human Rights to Communications Surveillance (2013), at 11 ("Integrity of Communications and Systems").

63. Data-sharing arrangements between law enforcement agencies, intelligence bodies and other State organs have also been found to raise necessity and proportionality concerns. According to the Office of the United Nations High Commissioner for Human Rights, data-sharing regimes that lack "use limitations", which ensure that the collection of data for one legitimate aim are not used for others, risk violating the right to privacy "because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purpose of another".[162]

64. In terms of the positive obligation of States to ensure human rights and protect individuals within their jurisdiction from human rights violations by third parties, Marko Milanovic has stated that this obligation would entail two main components in the surveillance context:[163]

> First, states would need to regulate private companies operating in areas under control that collect, store, process, or have access to personal data. This would include, but not necessarily be limited to, basic standards on data protection. Second, states would need to exercise due diligence and undertake all effective measures reasonably available to them to prevent interferences with privacy by third parties.

65. Finally, it is important to note that in October 2017, the Special Rapporteur on the Right to Privacy encouraged States to adopt a cyber surveillance treaty, submitting that "it is both possible and reasonable that a significant number of States will eventually coalesce around a legal instrument to regulate surveillance and protect privacy in cyberspace".[164]

---

[162] A/HRC/27/37, para. 27. See similarly, A/69/397, para. 56; and A/HRC/13/37, para. 50.

[163] Marko Milanovic, op. cit., page 123. See also, A/HRC/35/22, para. 17-22.

[164] A/HRC/34/60, at 21. See also, the public consultation co-organised by the EU-supported MAPPING Project and the United Nations Special Rapporteur for Privacy concerning new legal measures at international law intended to improve protection of privacy in the age of ubiquitous surveillance, including the possibility of development a multilateral international treaty on surveillance. Surveillance & Privacy—

A similar solution at the regional level has been proposed by the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe in 2015, which put forward a multilateral "no-spy" treaty with the aim of laying down rules governing cooperation for the purposes of combatting terrorism and organized crimes.[165] Although welcoming these developments, Eliza Watt has cautioned that "the first step towards achieving regulation of the working methods of intelligence agencies must be a clear articulation in law of what *is* cyber surveillance and cyber espionage".[166]

C. Data protection

66. Although the protection of personal data falls within the scope of the right to privacy,[167] in recent years data protection has increasingly been recognised as a distinct human right.[168] According to Kriangsak Kittichaisaree, data protection and the right to privacy may be distinguished on the basis that "[t]he former regulates the processing of an individual's personal data—be it private or non-private, whereas the latter protects an individual against intrusion into his private sphere".[169]

Considering New Measures at International Law, *Managing Alternatives for Privacy, Property and Internet Governance*, 22 May 2017.

[165] Parliamentary Assembly of the Council of Europe Resolution 2045, 21 April 2015.

[166] Eliza Watt, op. cit., 19 (emphasis in original).

[167] Human Rights Committee, 'General Comment No. 16—Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I), para. 10.

[168] See similarly, A/HRC/13/37, para. 12 (noting that "data protection is also emerging as a distinct human or fundamental right"); and A/HRC/17/27, para. 58 ("the protection of personal data represents a special form of respect for the right to privacy"). For a general overview of the international legal regulation of data protection, see generally, Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer, 2017), pages 57-83.

[169] Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer, 2017), at 59. See also, J. Kokott and C. Sobotta, *The Distinction between Privacy and Data Protection in the Jurisprudence*

67. In 2016, 111 countries worldwide had enacted data protection legislation,[170] much of which varies significantly on even the most basic elements of the protection of personal data.[171] As Christopher Kuner has observed, "considerable differences still exist in the approaches to data protection around the world, owing to cultural, historical, and legal factors".[172] In addition, at the international level, a range of binding and non-binding data protection instruments have also been enacted.[173]

68. In terms of binding instruments, a number of instruments have been enacted at both multilateral and regional levels.[174] At the multilateral level, the only treaty on data protection with a global scope of application open to any State is the Council of Europe Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).[175] The Convention obligates States Parties to legislate "for every individual, whatever his nationality or residence, respect for his

---

of the CJEU and the ECtHR (3 *International Data Privacy Law,* 2013) page 222.

170 Contribution by Eliza Watt, page 15.

171 Kriangsak Kittichaisaree, *op. cit.,* pages 57-58.

172 Christopher Kuner, *The European Union and the Search for an International Data Protection Framework* (2 Groningen Journal of International Law, 2014) page 59.

173 Ibid., at 58-59.

174 There have been growing calls for a stronger international legal framework for data protection See, for example, 27th International Conference of Data Protection and Privacy Commissioners, 'The Protection of Personal Data and Privacy in a Globalised World: a Universal Right respecting Diversities', 14-16 September 2005 (issuing the 'Montreaux Declaration', which appealed to the United Nations "to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights"); and Article 29 Working Party, 'The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data', WP 168, 1 December 2009, at 10 (stating that "global standards regarding data protection are becoming indispensable" and that it supports "the development of a global instrument providing for enforceable, high level privacy and data protection principles").

175 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature 28 January 1981; entered into force 1 October 1985 ETS 108.

rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection)".[176] An Additional Protocol to the Convention regarding Supervisory Authorities and Transborder Data Flows was introduced in 2001 to remedy several gaps in the original Convention, including the lack of rules on transborder data flows to third parties.[177]

69. At the regional level, Article 8 of the Charter of Fundamental Rights of the European Union recognises the protection of personal data as a human right.[178] In addition, various EU directives and regulations on data protection have also been adopted.[179] In this regard, a new General Data Protection Regulation will apply across all EU Member States from May 2018 with the aim of making Europe "fit for the

---

[176] Article 1, Convention 108.

[177] Contribution by Eliza Watt, page 17.

[178] Article 8, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02 ("(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."). See generally, Yvonne McDermott, *Conceptualising the right to data protection in an era of Big Data* (*Big Data & Society,* January-June 2017) page 1.

[179] See, in particular, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995; and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 27 April 2016. See also, *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, Court of Justice of the European Union, Judgment, 6 October 2015 (invalidating the European Commission's decision finding that the US ensured an adequate level of protection for the transfer of personal data under the Safe Harbour privacy principles).

digital age",[180] including through several provisions related to automated decision-making.[181] According to Christopher Kuner, EU data protection law is influential at the global level in two respects, "first, by serving as a model for the enactment of data protection law in other regions, and second, by its extraterritorial application to data processing in third countries".[182]

70. In terms of non-binding data protection instruments, relevant enactments include the United Nations General Assembly Resolution 45/95 on Guidelines for the Regulation of Computerized Personal Data Files,[183] the International Law Commission's syllabus on Protection of Personal Data in Transborder Flow of Information,[184] the Inter-American Juridical Committee's Proposed Statement of Principles for Privacy and Personal Data Protection in the Americas,[185] the Tshwane

---

[180] European Commission, Reform of EU Data Protection Rules (2017), accessible online at: http://ec.europa.eu/justice/data-protection/reform/.

[181] See generally, Andrew D. Selbst and Julia Powles, *Meaningful Information and the Right to Explanation* (7 International Data Privacy Law, 2017); and Bingham Centre for the Rule of Law, *Artificial Intelligence, Big Data and the Rule of Law: Event Report* (9 October 2017).

[182] Christopher Kuner, op. cit., page 60. See similarly, Kriangsak Kittichaisaree, *op. cit.,* 60-61; and Maria Tzanou, *European Union Regulation of Transatlantic Data Transfers and Online Surveillance* (17 Human Rights Law Review, 2017), page 552 (noting how the EU's Data Protection Directive has been characterised as "gunboat diplomacy" to the extent that it has "prompted many countries to change their data protection rules—or indeed introduce new ones—in order to be able to receive data transfers from the EU").

[183] A/RES/45/95.

[184] 'Report of the International Law Commission', 58th Session (1 May–9 June and 3 July–11 August 2006), General Assembly Official Records, 61st Session Supplement No. 10, A/61/10, at 498 ("The international binding and non-binding instruments, as well as the national legislation adopted by States, and judicial decisions reveal a number of core principles, including: (a) lawful and fair data collection and processing; (b) accuracy; (c) purpose specification and limitation; (d) proportionality; (e) transparency; (f) individual participation and in particular the right to access; (g) non-discrimination; (h) responsibility; (i) supervision and legal sanction; (j) data equivalency in the case of transborder flow of personal data; (k) the principle of derogability.")

[185] Inter-American Juridical Committee, Organisation of American States, Proposed Statement of Principles for Privacy and Personal Data

Principles,[186] the Organisation for Economic Co-operation and Development's (OECD) Privacy Guidelines,[187] the Asia-Pacific Economic Cooperation's (APEC) Privacy Framework,[188] and the Economic Community of West African States' (ECOWAS) Supplementary Act on Personal Data Protection.[189]

71. In order for States to improve upon this diverse normative framework of data protection, two paths forward have been identified.[190] First, States should devote greater efforts to "mapping areas of convergence between standards in different legal systems".[191] According to Kittichaisaree and Kuner, this approach would enable "different approaches to data protection to develop naturally, with international cooperation producing interfaces that allow them to gradually grow closer together

---

Protection in the Americas, OEA/Ser.Q CJI/RES.186 (LXXX-O/12), 9 March 2012 (listing the following principles: (a) lawful and fair purposes; (b) clarity and consent; (c) relevant and necessary; (d) limited use and retention; (e) duty of confidentiality; (f) protection and security; (g) accuracy of information; (h) access and correction; (i) sensitive information; (j) accountability; (k) trans-border ow of information and accountability; and (l) disclosing exceptions).

186 The Global Principles on National Security and the Right to Information (Tshwane Principles) (Open Society Foundations, 12 June 2013).

187 OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data', *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL as amended on 11 July 2013 by C(2013)79, Annex (2013) (recognising the following basic principles of national application: (a) collection limitation principle; (b) data quality principle; (c) purpose specification principle; (d) use limitation principle; (e) security safeguards principle; (f) openness principle; (g) individual participation principle; (h) accountability principle).

188 APEC Privacy Framework (APEC Secretariat, 2005) (recognising the following privacy principles: (a) preventing harm; (b) notice; (c) collection limitations; (d) uses of personal information; (e) choice; (f) integrity of personal information; (g) security safeguards; (h) access and correction; and (i) accountability).

189 ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection, 37th Session of the Authority of Heads of State and Government, Abuja, 16 February 2010.

190 Kriangsak Kittichaisaree and Christopher Kuner, 'The Growing Importance of Data Protection in Public International Law', *EJIL Talk!*, 14 October 2015.

191 Christopher Kuner, op. cit., page 67.

over time".[192] Second, in the longer term, States should consider developing an international agreement on data protection with the aim of elaborating a clear and uniform legal framework. According to Eliza Watt, the new Draft Modernized Convention 108,[193] which was published in September 2016, represents "perhaps the only prospect for a universal standard in the field of data privacy" for this purpose.[194]

D. Encryption and anonymity

72. Encryption—a mathematical process that scrambles data in order to protect the confidentiality and integrity of content against third party access or manipulation—has become an increasingly common means of digital security.[195] Encryption may be applied to data in transit—such as email or messages—and data at rest—such as data stored on hard drives, tablets, mobile phones or cloud services.[196]

---

[192] Kriangsak Kittichaisaree and Christopher Kuner, op. cit..

[193] Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, September 2016, available online at: https://rm.coe.int/16806a616c.

[194] Eliza Watt, 'Right to Privacy', *Open Consultation on United Nations GGE 2015 Norm Proposals* (2017), page 18. See similarly, Christopher Kuner, op. cit., page 66 ("the Council of Europe Convention 108 presents perhaps the best treaty-based possibility for the adoption of an international data protection framework").

[195] A/HRC/29/32, para. 1 and 7; and United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (United Nations 2012), para. 194. See, however, Berkman Center for Internet & Society, op. cit., page 3 (arguing that intelligence agencies will have access to significant unencrypted data in the future because encryption technologies are unlikely to be adopted ubiquitously by companies, software ecosystems tend to be fragmented, networked sensors and the Internet of Things may enable real-time intercept and recording with after-the-fact access, and metadata is not encrypted and the vast majority is likely to remain so).

[196] A/HRC/29/32, para. 1 and 7. See also, Amnesty International, *A Matter of Human Rights* (March 2016), pages 6-8 (distinguishing between three types of encryption: (a) full-disk or device encryption; (b) end-to-end encryption; and (c) transport encryption or transport layer encryption)

73. Importantly, encryption protects the content of communications, but not metadata.[197] As such, in order to conceal one's online identity, individuals have turned to a number of anonymising tools such as virtual private networks (VPNs), proxy services, networks and software, and peer-to-peer networks.[198]

74. According to the United Nations Special Rapporteur on Freedom of Expression, there are two sides to encryption and anonymity.[199] On the one hand, encryption and anonymity shield opinions and beliefs from outside scrutiny and surveillance, as well as empowering individuals to circumvent State-imposed barriers to information and ideas. They also provide law enforcement with valuable tools to ensure operational security in undercover operations, as well as empowering vulnerable groups to ensure their privacy in the face of harassment. On the other hand, encryption and anonymity may be used by terrorists and ordinary criminals to hide their activities, while harassment and cyberbullying may rely on anonymity as a mask for discrimination.[200] In the face of such challenges, however, the Special Rapporteur has also noted that "Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism".[201]

---

197 A/HRC/29/32, para. 9.

198 Amnesty International, *op. cit., page* 8; A/HRC/29/32, para. 9; and United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (United Nations 2012), para. 195-197.

199 A/HRC/29/32, para. 12-13. For a useful overview of the discourse on encryption from different international legal perspectives, see generally, Ashley Deeks, *The International Legal Dynamics of Encryption* (Hoover Institution Essay, Series Paper No 1609, 2016); and Amnesty International, *op. cit*.

200 On the use of encryption and anonymising tools for terrorist purposes, see generally, Counter-Terrorism Implementation Task Force (CTITF), *Countering the Use of the Internet for Terrorist Purposes—Legal and Technical Aspects* (CTITF Publication Series, May 2011), paras 17-23.

201 A/HRC/29/32, para. 13.

75. Since encryption and anonymity establish "a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks",[202] any restrictions on such tools must comply with international human rights law. In particular, any restriction must not interfere with the right to hold opinions, whilst any restriction that limits the rights to privacy and freedom of expression must be provided by law, imposed to achieve a legitimate aim, and be necessary and proportionate.[203]

76. Bearing in mind the obligations of States to respect and protect the rights to privacy, freedom of opinion, and freedom of expression, the United Nations Special Rapporteur on Freedom of Expression has identified particular types of regulations of encryption technology and anonymising security tools that fail to meet the requisite standards of international human rights law.[204]

---

[202] A/HRC/29/32, para. 16. See generally, Article 19 ICCPR; Article 10 ECHR; Article 13 ACHR; Article 9 ACHPR; Human Rights Committee, 'General Comment No. 34—Freedom of Opinion and Expression', ICCPR 12 September 2011, Document CCPR/C/GC/34; and Michael N. Schmitt (ed.), op. cit., pages 187-189.

[203] See generally, A/HRC/29/32, para. 16-26 and 29-35; and 'Promoting Strong Encryption and Anonymity in the Digital Age', Joint Civil Society Statement submitted to the 29th Session of the United Nations Human Rights Council, 17 June 2015. Treaties have set forth the permissible limitations on the right to freedom of expression using slightly variable language. See, for example, Article 19(3) ICCPR (referring to the rights or reputations of others, the protection of national security or of public order or of public health or morals); and Article 10(2) EHCR (referring to national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, preventing the disclosure of information received in confidence, or maintaining the authority and impartiality of the judiciary); and Article 13(2)-(5) ACHR (referring to respect for the rights or reputations of others; the protection of national security, public order, or public health or morals; the moral protection of childhood and adolescence; and countering propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence).

[204] A/HRC/29/32, para. 36-55. See similarly, Amnesty International, *op. cit., pages* 25-40; and Global Commission of Internet Governance, *One*

77. Outright prohibitions on the individual use of encryption technology, as well as State regulations that are tantamount to a ban—such as rules requiring licences for encryption use, setting weak technical standards for encryption, controlling the import and export of encryption tools, or penalizing those who produce and distribute encryption tools—constitute disproportionate restrictions on privacy and freedom of expression. These types of regulations should be avoided because they "deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends".[205]

78. Regulations that mandate the implementation of so-called back-door access in commercial products, requiring developers to install vulnerabilities that enable State access to encrypted communications or a key escrow system that requires users to store their private keys with the State or a trusted third party, also constitute disproportionate restrictions on privacy and freedom of expression. These types of regulations should be avoided because "intentional flaws invariably undermine the security of all users online, since a backdoor, even if intended solely for government access, can be accessed by unauthorized entities, including other States or non-State actors".[206] Moreover, "measures that impose generally applicable restrictions on

---

Internet (Centre for Governance Innovation and Chatham House, 2016), pages 33-34.

[205] A/HRC/29/32, para. 40. See also, A/HRC/31/64, para. 19-27 (identifying the question of whether a smartphone should be considered a compellable witness as a subject for further investigation); and Amnesty International, *op. cit., page* 38.

[206] A/HRC/29/32, para. 42 and 44 ("the key escrow system depends on the integrity of the person, department or system charged with safeguarding the private keys, and the key database itself could be vulnerable to attack, undermining any user's communication security and privacy"). See also, A/71/373, para. 20; A/HRC/32/38, para. 62; A/HRC/35/22, para. 21; A/HRC/31/64, para. 30-31 (welcoming the decision of the Dutch government to formally oppose the introduction of backdoors in encryption products); A/HRC/32/38, para. 30-32; and Amnesty International, *op. cit.*, pages 38-40.

massive numbers of persons, without a case-by-case assessment, would almost certainly fail to satisfy proportionality".[207]

79. Court-ordered decryption may only be permissible when it results from "transparent and publicly accessible laws applied solely on a targeted case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals".[208]

80. Outright prohibitions of anonymity online, as well as regulations that are tantamount to bans on anonymity—such as requiring real-name registration for access to digital communications or online services, requiring SIM card registration for mobile users, or denying access to anonymity tools such as Tor, proxies and VPNs—fail to satisfy the conditions of necessity and proportionality.[209] According to the United Nations Special Rapporteur on Freedom of Expression, "restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas" and "can also result in individuals' de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities".[210]

E. Access to content online

81. As the Internet has emerged as a vital medium for individuals to exercise their right to freedom of opinion and expression, the issue of access to online content has become a topic of growing concern within the international community. According to the United Nations Special Rapporteur on Freedom of Expression, "as a general rule, there should be as little restriction as possible to the flow of information on the Internet, except under a few, very exceptional and limited

---

[207] A/HRC/29/32, para. 43.

[208] A/HRC/29/32, para. 60. See similarly, 'Promoting Strong Encryption and Anonymity in the Digital Age', Joint Civil Society Statement submitted to the 29th Session of the United Nations Human Rights Council, 17 June 2015; and Amnesty International, *op. cit.,* pages 39-40.

[209] A/HRC/29/32, para. 49, 50-53 and 60. See also, A/HRC/23/40, para. 68-70.

[210] A/HRC/23/40, para. 49.

circumstances prescribed by international law for the protection of other human rights".[211] This perspective reflects the importance of the rights to freedom of opinion and expression not only on their own accord but also as "an 'enabler' of other rights, including economic, social and cultural rights, such as the right to education and the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications, as well as civil and political rights, such as the rights to freedom of association and assembly".[212]

82. According to the Rabat Plan of Action, adopted by experts following a series of consultations convened by the Office of the United Nations High Commissioner for Human Rights, a clear distinction should be drawn between three types of expression:[213] (a) expression that constitutes a criminal offence; (b) expression that is not criminally punishable, but may justify a civil suit or administrative sanctions; and (c) expression that does not give rise to criminal, civil or administrative sanctions, but still raises concern in terms of tolerance, civility and respect for the rights of others.

83. States are required to prohibit the following exceptional types of expression, taking care to ensure that the prohibition is formulated with sufficient precision by law, in pursuit of a legitimate aim, and in conformity with the tests of necessity and proportionality:[214] (a) child pornography;[215] (b) direct and public incitement to commit genocide;[216] (c) advocacy of national, racial or religious hatred that constitutes incitement

---

[211] A/66/290, para. 12.

[212] A/HRC/17/27, para. 22.

[213] Rabat Plan of Action on the Prohibition of Advocacy of National, Racial or Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence, A/HRC/22/17/Add.4, Appendix, 5 October 2012, para. 20.

[214] For discussion of these categories of expression, see generally, A/66/290, para. 20-36.

[215] See, in this regard, Article 3(1)(c), Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

[216] See, in this regard, Article 3(c), Convention on the Prevention and Punishment of the Crime of Genocide.

to discrimination, hostility or violence;[217] and (d) incitement to terrorism.[218]

84. Given the absence of agreed definitions of advocacy of hatred and incitement to terrorism under international law, a number of experts have provided guidance on how States should understand these terms in practice.

85. With respect to advocacy of hatred, the Rabat Plan of Action proposed a six-part threshold test for expressions considered as criminal offences:[219]

- **Context**: Placing the speech act within the social and political context prevalent at the time the speech was made and disseminated;
- **Speaker**: Examining the speaker's position or status in the society, with particular emphasis on the individual's or organisation's standing in the context of the audience to whom the speech is directed;
- **Intent**: Identifying the intent of the speaker to engage in advocacy of hatred;
- **Content and form**: Examining the degree to which the content of the speech was provocative and direct, as well

---

[217] See, in this regard, Article 20(2), ICCPR; Article 4, International Convention on the Elimination of All Forms of Racial Discrimination; Human Rights Committee, 'General Comment No. 34—Freedom of Opinion and Expression', ICCPR 12 September 2011, Document CCPR/C/GC/34, para. 50-52; and 'Report of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 7 September 2012, A/67/357.

[218] See, in this regard, United Nations Security Council Resolution 1624, 14 September 2005, S/RES/1624 (2005); 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', 22 December 2010, U.N. Doc A/HRC/16/51, paras 29-32; and 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism', 29 April 2016, A/HRC/31/65, paras 23-24.

[219] Rabat Plan of Action on the Prohibition of Advocacy of National, Racial or Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence, A/HRC/22/17/Add.4, Appendix, 5 October 2012, para. 29. See similarly, A/67/357, para. 46.

as the form, style, nature of arguments deployed in the speech or the balance struck between arguments deployed;

- **Extent of the speech act**: Examining the reach of the speech act, its public nature, its magnitude and size of its audience; and
- **Likelihood, including imminence**: Identifying whether there was a reasonable probability that the speech would succeed in inciting actual action against the target group.

86. With respect to incitement to terrorism, the United Nations Special Rapporteur on Counter-Terrorism has formulated the following model offence: "it is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed".[220] In addition, the Special Rapporteur has emphasised that any domestic criminal laws that prohibit incitement to terrorism: "(a) must be limited to the incitement to conduct that is truly terrorist in nature […]; (b) must restrict the freedom of expression no more than is necessary for the protection of national security, public order and safety or public health or morals; (c) must be prescribed by law in precise language, including by avoiding reference to vague terms such as 'glorifying' or 'promoting' terrorism; (d) must include an actual (objective) risk that the act incited will be committed; (e) should expressly refer to two elements of intent, namely intent to communicate a message and intent that this message incite the commission of a terrorist act; and (f) should preserve the application of legal defences or principles leading to the exclusion of criminal liability by referring to 'unlawful' incitement to terrorism".[221]

87. At the other end of the spectrum, the Human Rights Council has stipulated that the following types of expression

[220] A/HRC/16/51, para. 32. See also, the Special Rapporteur's model definition of terrorism at para. 28.

[221] A/HRC/16/51, para. 31.

should never be subject to restrictions:[222] (a) discussion of government policies and political debate; (b) reporting on human rights, government activities and corruption in government; (c) engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy; and (d) expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups.

88. Between these two poles, there are other forms of hate speech that target identifiable individuals but do not necessarily advocate hatred to a broader audience with the purpose of inciting discrimination, hostility or violence. Examples of these types of expression include discriminatory threats of unlawful conduct, discriminatory harassment, and discriminatory assault. States *may* prohibit these types of expression provided they do so with sufficient precision by law, in pursuit of a legitimate aim, and in conformity with the conditions of necessity and proportionality.[223]

89. According to the Rabat Plan of Action, "[c]riminal sanctions related to unlawful forms of expression should be seen as last resort measures to be applied only in strictly justifiable situations".[224] In particular, defamation should be decriminalized,[225] while offences that seek to criminalize extremist speech that does not amount to incitement should be avoided.[226]

90. The right to freedom of expression also implies that it should be possible "to scrutinize, openly debate and criticize, even harshly and unreasonably, ideas, opinions, belief systems

---

[222] A/HRC/12/16, 2 October 2009, A/HRC/12/16, para. (p) (i). See similarly, A/66/290, para. 43 (referring to the findings of the Human Rights Committee that the legitimate aims listed in Article 19(3) of the ICCPR may never be invoked to justify "muzzling of any advocacy of multi-party democracy, democratic tenets and human rights").

[223] Article 19, 'Germany: Draft Bill on the Improvement of Enforcement of Rights in Social Networks: Legal Analysis', April 2017, at 8.

[224] A/HRC/22/17/Add.4, Appendix, 5 October 2012, para. 34.

[225] A/HRC/17/27, para. 36.

[226] A/HRC/31/65, para. 39.

and institutions, including religious ones, as long as this does not advocate hatred that incites hostility, discrimination or violence against an individual or a group of individuals".[227] According to the United Nations Special Rapporteur on Freedom of Expression, "for the types of expression that do not rise to criminal or civil sanctions, but still raise concerns in terms of civility and respect for others, effort should be focused on addressing the root causes of such expression, including intolerance, racism and bigotry by implementing strategies of prevention".[228] In such circumstances, the strategic response to expressions deemed offensive or intolerant should be "more speech: more speech that educates about cultural differences; more speech that promotes diversity and understanding; more speech to empower and give voice to minorities and indigenous peoples, for example through the support of community media and their representation in mainstream media".[229]

91. In terms of the different forms that state regulations concerning access to online content may take, a range of experts have concluded that the use of communications "kill switches" to shut down entire parts of a network or service can never constitute a justifiable restriction on the right to freedom of expression.[230]

92. Similarly, a number of experts have found that the use of blocking or filtering techniques are frequently in violation of the right to freedom of expression on the basis that either the specific conditions that justify blocking or filtering are not established in law, the blocking or filtering are not justified to pursue a legitimate aim, they are an unnecessary or disproportionate means to achieve the purported aim because they are not sufficiently targeted and render a wide range of

---

[227] A/66/290, para. 30.

[228] A/66/290, para. 40.

[229] A/66/290, para. 41.

[230] Joint Declaration on Freedom of Expression and Responses to Conflict Situation, 4 March 2015, para. 4(c); 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 11 May 2016, A/HRC/32/38, para. 48; and A/HRC/35/2, para. 8-16.

content inaccessible beyond that which has been deemed illegal, or they are not subject to the intervention of or possibility for review by a judicial or independent body.[231]

93. Private Internet intermediaries—including web hosting companies, Internet service providers, search engines and social media platforms—serve as an important gateway for people to access the Internet and in transmitting third-party content. To the extent that States require the assistance of private intermediaries to restrict access to content online, a number of experts have concluded that:

- Censorship measures should never be delegated to private entities.[232]
- Intermediaries should never be held liable for refusing to take action that infringes the human rights of individuals.[233]
- "Intermediaries should never be liable for any third-party content […] unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that".[234]

---

[231] A/HRC/17/27, para. 31; and A/HRC/32/38, para. 39 and 45-47.

[232] A/HRC/17/27, para. 75; and Article 19, *Internet Intermediaries: Dilemma of Liability* (Article 19, 2013), at 16.

[233] A/HRC/17/27, para. 75.

[234] Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, adopted by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, 3 March 2017, para. 1(d). See also, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commercial, in the Internal Market (shielding intermediaries from liability for illegal third-party content where the intermediary lacks actual knowledge of the illegal activity or information and, upon obtaining knowledge, acts expeditiously to remove access to the information, as well as prohibiting States from imposing general obligations on intermediaries to monitor activity on

- Any requests submitted to intermediaries to prevent access to content should be conducted through "an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences".[235]
- Notice and takedown frameworks may be contrary to the right to freedom of expression to the extent that they incentivize "questionable claims" to remove online content and fail to provide "adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation".[236]

94. Finally, in addition to ensuring the availability of content online, it is also important that States ensure that individuals possess the necessary "digital literacy" to make full use of the Internet.[237] According to the Global Commission on Internet Governance, States should promote digital literacy programs in schools and government organisations so as to enable

---

their services); and Article 19, *Internet Intermediaries: Dilemma of Liability* (Article 19, 2013), at 16. See, however, *Delfi AS v. Estonia*, Application No. 64569/09, European Court of Human Rights, Judgment, 16 June 2015 (concluding that the imposition of civil liability by a national court on an online news portal for failing to remove "clearly unlawful" comments posted to its website by an anonymous third party did not violate Article 10 of the ECHR, even without notice being provided). On the development of the jurisprudence of the European Court of Human Rights with respect to intermediary liability in this context, see generally, Robert Spano, *Intermediary Liability for Online User Comments under the European Convention on Human Rights* (17 *Human Rights Law Review,* 2017), page 665; Article 19, 'Germany: Draft Bill on the Improvement of Enforcement of Rights in Social Networks: Legal Analysis', April 2017; and Lisl Brunner, *The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v. Estonia* (16 *Human Rights Law Review,* 2016), page 163.

235 A/HRC/17/27, para. 75. See similarly, A/HRC/32/38, para. 85; and Article 19, *Internet Intermediaries: Dilemma of Liability* (Article 19, 2013), at 16.

236 A/HRC/32/38, para. 43. See also, Article 19, *Internet Intermediaries: Dilemma of Liability* (Article 19, 2013), at 16-17 (proposing "notice-to-notice procedures" for civil claims relating to copyright, defamation, privacy, adult content and bullying as an alternative to "notice and take down procedures").

237 A/66/290, para. 45-60.

individuals to understand "the foundations of the technology and the principles that must be maintained to preserve the Internet as a tool for innovation, communication, and the enjoyment of rights".[238]

95. Similarly, the United Nations Special Rapporteur on Freedom of Expression has encouraged States to provide support for training in ICT skills, including explaining the benefits of accessing information online, clarifying how to responsibly contribute information online, as well as teaching about Internet safety and security.[239] In addition, the Special Rapporteur has called upon States to empower marginalized groups by ensuring that they receive effective digital literacy training, emphasizing the potential of the Internet to enable "people who are disadvantaged, discriminated against or marginalized to obtain information, assert their rights and participate in the public debate concerning social and political changes", as well as empower "minorities and indigenous peoples to express and reproduce their cultures, language and traditions, preserving their heritage and making a valuable contribution to others in a truly multicultural world".[240] For this purpose, the Special Rapporteur has outlined principles and measures that States should follow to ensure that persons with disabilities have full and effective use of the Internet, language barriers are reduced, and gender inequalities in terms of access to content online are overcome.[241]

---

[238] Global Commission on Internet Governance, *One Internet* (Centre for International Governance Innovation and The Royal Institute for International Affairs, 2016), page 25.

[239] A/66/290, at pars 45- 47 and 88.

[240] A/66/290, para. 48.

[241] A/66/290, para. 49-60 and 87. See also, Target 5.b, United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*, A/RES/70/1 ("Enhancing the use of enabling technology, in particular information and communications technology, to promote the empowerment of women"); and Global Commission on Internet Governance, *One Internet* (Centre for International Governance Innovation and The Royal Institute for International Affairs, 2016), at 26-27 (identifying various measure to encourage an inclusive Internet, including for persons with disabilities and refugees).

96. Finally, according to the World Bank, digital literacy programs considered most successful have the following principles in common:[242]

- They are mainstreamed into the non-ICT curriculum, emphasizing ICTs as a tool rather than a subject.
- They focus on teachers' digital literacy.
- They go beyond ICTs, into the beginnings of "computational thinking", namely the problem-solving skills and techniques used by software engineers to write programs.
- They are embedded in local content, connecting learners to issues relevant to them as well as reducing language barriers.

F. Access to Internet infrastructure

97. With over half of the world's population still offline, the benefits of the Internet are unevenly distributed.[243] According to the Global Commission on Internet Governance, "[i]f the rest of humanity is not given the opportunity to come online, digital and physical divides both within and between societies will widen, locking some into a permanent cycle of exclusion from an increasingly digital global economy".[244] A range of factors have been identified to explain ongoing hurdles to the spread of Internet access, including "continued policy failures such as regulatory capture, troubled privatizations, inefficient spectrum

---

[242] World Bank, *World Development Report 2016: Digital Dividends* (World Bank, 2016), page 265.

[243] World Bank, *World Development Report 2016: Digital Dividends* (World Bank, 2016), page 200; and Global Commission on Internet Governance, *One Internet* (Centre for International Governance Innovation and The Royal Institute for International Affairs, 2016), page viii.

[244] Global Commission on Internet Governance, *One Internet* (Centre for International Governance Innovation and The Royal Institute for International Affairs, 2016), page viii. See similarly, A/66/290, para. 64; and A/HRC/17/27, para. 60-62.

management, excessive taxation of the sector, and monopoly control of international gateways".[245]

98. Although access to the Internet is not a human right as such under customary or conventional international law,[246] the United Nations Special Rapporteur on Freedom of Expression has emphasised that "States have a positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, which includes the Internet".[247] Similarly, the United Nations Human Rights Committee has explained that States Parties to the ICCPR "should take all necessary steps to foster the independence of […] new media and to ensure access of individuals thereto".[248] Beyond the right to freedom of expression, it is important to emphasise that the Internet is also essential for the enjoyment of other rights, including the right to education, the right to freedom of association and assembly, the right to full participation in social, cultural and political life and the right to social and economic development.[249]

99. Against this background, the United Nations Special Rapporteur on Freedom of Expression has called upon States to develop "a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet

---

[245] World Bank, *World Development Report 2016: Digital Dividends* (World Bank, 2016), page 25.

[246] See, in this regard, A/66/290, para. 61 ("access to the Internet is not yet a human right as such"); Michael N. Schmitt (ed.), *op. cit.,* page 195 ("'access to the Internet' is also not an international human right in itself as a matter of customary international law; technology is an enabler of rights, not a right as such"); and Stephen Tully, *A Human Right to Access the Internet? Problems and Prospects* (14 *Human Rights Law Review,* 2014), page 194.

[247] A/66/290, para. 61.

[248] Human Rights Committee, 'General Comment No. 34—Freedom of Opinion and Expression', ICCPR 12 September 2011, Document CCPR/C/GC/34, para. 15.

[249] A/66/290, para. 61.

widely available, accessible and affordable to all segments of population".[250]

100. To this end, a range of guidance has been developed on how States can promote universal access to the Internet in practice.[251] First, States have been called upon to put in place "measures to encourage competition and foster investment in networks as fundamental requirements in any effort to enable access and promote development", facilitate network sharing, and invest in public access points in schools, libraries and other social service venues to provide wider access to communities that would otherwise be cut off from the Internet due to factors such as income or geography.[252] Second, States have been called upon to ensure that their taxation policies "do not bias the market for Internet services or related equipment", as well as to use the tools at their disposal "to promote competition among the producers and sellers of devices to increase affordability, whether purchased separately or as part of service plan".[253] Third, a number of experts have called upon States to respect network neutrality—the principle that all Internet data should be treated equally without undue interference—by prohibiting "attempts to assign priority to certain types of Internet content

---

[250] A/HRC/17/27, para. 85. See similarly, World Summit on the Information Society, Geneva Declaration of Principles, 12 December 2003, WSIS-03/GENEVA/DOC/004, para. 1; World Summit on the Information Society, Tunis Commitment, 18 November 2005, WSIS-05/TUNIS/DOC/7, para. 2; and Global Commission on Internet Governance, *op. cit.*, page 15.

[251] For examples of international and national initiatives aimed at addressing the digital divide, see generally, A/HRC/17/27, para. 63-65; and A/66/290, para. 68-74.

[252] Global Commission on Internet Governance, *One Internet* (Centre for International Governance Innovation and The Royal Institute for International Affairs, 2016), at 20.

[253] Global Commission on Internet Governance, *op. cit.*, page 23. See also, World Bank, *World Development Report 2016: Digital Dividends* (World Bank, 2016), pages 25 and 204-221 (elaborating a supply-side ICT policies to improve the availability, accessibility and affordability of the Internet across the ICT value chain, which "stretches from the point where the internet enters a country (the first mile), passes through that country (the middle mile) to reach the end user (the last mile), and certain hidden elements in between (the invisible mile)").

or applications over others for payment or other commercial benefits".[254] Fourth, States—in conjunction with business enterprises and civil society organizations—have also been called upon to bridge the gender digital divide by ensuring that ICTs are accessible to women on an equal basis without discrimination and by promoting women's equal, effective and meaningful participation online.[255] Finally, States have also been called upon to honour their commitment, expressed in Target 9.c of the Sustainable Development Goals,[256] to facilitate technology transfer to developing States and to integrate effective programmes to facilitate universal access to the Internet in their development and assistance policies.[257]

Recommendations

101. Based on the preceding analysis, the following conclusions and recommendations are put forward to guide states in their implementation of recommendation 13 (e) in the GGE 2015 Report.

A. Scope of application

- States are under a negative obligation to *respect* human rights, as well as a positive obligation to *protect* them.

---

[254] A/HRC/35/2, para. 23-28 and 80. See also, Global Commission on Internet Governance, *One Internet* (Centre for International Governance Innovation and The Royal Institute for International Affairs, 2016), at 21-22 (raising a number of concerns with "zero-rated content").

[255] 'Report of the UN High Commissioner for Human Rights on Promotion, Protection and Enjoyment of Human Rights on the Internet: Ways to Bridge the Gender Digital Divide from a Human Rights Perspective', 5 May 2017, U.N.Doc. A/HRC/35/9.

[256] Target 9.c, United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*, A/RES/70/1 ("Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020").

[257] 'Report of the United Nations Special Rapporteur on the Promotion and Enjoyment of the Right to Freedom of Opinion and Expression', 16 May 2011, A/HRC/17/27, para. 86.

- States are required to satisfy their negative and positive obligations to respect and protect the human rights of all persons on their territory, as well as persons located in territories under a State's effective control.
- States are required to satisfy their negative obligation to respect the human rights of all persons within their power or effective control. In such circumstances, only those specific rights relevant to the situation will be engaged and "control" should be understood to mean not only physical control but also control over an individual's rights.
- It remains a matter of contention whether States must satisfy their positive obligation to protect the human rights of individuals under their power or effective control. In any case, States will generally need effective control over a territory in order to comply with their positive obligations in practice.
- States are required to take reasonable measures to prevent the occurrence of reasonably foreseeable human rights violations that occur outside their territories due to the activities of business entities over which they can exercise control. Reasonable measures include requiring corporations to deploy their best efforts to ensure that entities whose conduct those corporations may influence respect human rights, as well as putting in place appropriate monitoring and accountability procedures to ensure prevention and enforcement. Reasonable measures should also encourage corporations over which States can exercise control to adopt generally acceptable international standards of corporate social responsibility, and oversee self-regulation, private ordering and coding by corporate actors.

B. Surveillance

- States are required to ensure that the design and implementation of surveillance programmes conform with the requirements of international human rights law, in particular the right to privacy as defined in customary

international law and—if the State is party to a relevant treaty—conventional international law.

- Privacy is a broad concept encompassing the integrity and confidentiality of both the content of communications—including all forms of correspondence and personal information—and metadata. The transmission of personal data to and use by other authorities, which enlarges the group of persons with knowledge of the data intercepted, constitutes a further separate interference with an individual's privacy. In addition, the mere existence of legislation which allows a system for the secret monitoring of communications amounts in itself to an interference with privacy.
- States are required to ensure that any interference with an individual's privacy through surveillance practices has a basis in domestic law, which must possess certain qualities:
  - States are required to ensure that the domestic law is accessible to the public, provides individuals with an adequate indication of the circumstances in which and the conditions on which public authorities are empowered to resort to surveillance measures, and identifies the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.
  - States should ensure that the domestic law identifies the nature of offences that may give rise to an interception order, a definition of the categories of people liable to be subject to the surveillance measures, a limit on the duration of the surveillance measures, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which the data may or must be erased or destroyed.

  - States must establish effective procedural safeguards including effective, adequately resourced institutional arrangements, which may take the form of independent prior authorization and/or subsequent independent review of the surveillance measures.
  - States are required to ensure that victims of privacy violations have access to an effective remedy, including through the provision of an independent mechanism capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process guarantees, which has power to grant a binding remedy (including, where appropriate, an order for the cessation of surveillance or the destruction of the product). States should also provide information about interception of communications and available remedies to the persons concerned as soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure.
  - In conformity with the principle of non-discrimination, States are required to afford the same protection and safeguards to nationals and non-nationals, and to those within and outside their jurisdiction.
  - States are required to ensure that intelligence-sharing arrangements are conducted pursuant to a publicly accessible legal framework that complies with the above safeguards.
- States are required to justify any interference with an individual's privacy through surveillance measures on the basis of a legitimate aim, including such grounds as national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others.

- States must ensure that any interference with an individual's privacy through surveillances measures is a necessary and proportionate means to achieving the legitimate aim. In the surveillance context, this requires that the entity competent to authorize the surveillance be independent and capable of verifying the existence of a reasonable suspicion against the person concerned, in particular whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. In addition, the interception authorisation must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information.
- Based on the above requirements, States should avoid:
  - Mass or bulk surveillance programmes that permit public authorities to have access on a generalized basis to the content of electronic communications.
  - Mandatory third-party data retention programmes that require Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access.
  - Data-sharing arrangements between law enforcement agencies, intelligence bodies and other State organs that lack use limitations.

C. Data protection

- States must comply with applicable data protection regimes at the domestic, regional and multilateral levels and should seek to act in conformity with the standards and principles established by the various non-binding data-protection instruments that have been adopted.

- States should devote resources to mapping areas of convergence between data protection standards in different legal systems.
- States should consider developing an international agreement on data protection with the aim of elaborating a clear and uniform legal framework.

D. Encryption and anonymity

- Any restriction on encryption and/or anonymising technology must not interfere with the right to hold opinions, whilst any restriction that limits the rights to privacy and freedom of expression must be provided by law, imposed to achieve a legitimate aim, and be necessary and proportionate.
- States are required to avoid outright prohibitions on the individual use of encryption technology, as well as State regulations that are tantamount to a ban, because such prohibitions constitute disproportionate restrictions on privacy and freedom of expression.
- States are required to avoid regulations that mandate the implementation of back-door access in commercial products because such regulations constitute unnecessary and disproportionate restrictions on privacy and freedom of expression.
- Court-ordered decryption is only permissible when it results from transparent and publicly accessible laws applied solely on a targeted case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.
- States are required to avoid prohibitions of anonymity online, as well as State regulations that are tantamount to bans on anonymity, because such prohibitions constitute unnecessary and disproportionate restrictions on privacy and freedom of expression.

E. Access to content online

- As a general rule, there should be as little restriction as possible to the flow of information on the Internet, except under a few, very exceptional and limited circumstances prescribed by international law for the protection of other human rights.
- States are required to prohibit child pornography, direct and public incitement to commit genocide, advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, and incitement to terrorism, taking care to ensure that the prohibition is formulated with sufficient precision by law, in pursuit of a legitimate aim, and in conformity with the tests of necessity and proportionality. For the purpose defining prohibitions of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, as well as incitement to terrorism, States should be guided by the Rabat Plan of Action and the guidance of the United Nations Special Rapporteurs on Counter-Terrorism and Freedom of Expression.
- States may only prohibit other forms of hate speech that target identifiable individuals but do not necessarily advocate hatred to a broader audience with the purpose of inciting discrimination, hostility or violence, provided they do so with sufficient precision by law, in pursuit of a legitimate aim, and in conformity with the conditions of necessity and proportionality. In this regard, criminal sanctions related to unlawful forms of expression should be seen as last resort measures to be applied only in strictly justifiable situations.
- States are required to avoid restricting discussion of government policies and political debate, reporting on human rights, government activities and corruption in government, engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy, and expression of opinion and dissent,

religion or belief, including by persons belonging to minorities or vulnerable groups. The right to freedom of expression also implies that it should be possible to scrutinize, openly debate and criticize, even harshly and unreasonably, ideas, opinions, belief systems and institutions, including religious ones, as long as this does not advocate hatred that incites hostility, discrimination or violence against an individual or a group of individuals. For the types of expression that do not rise to criminal or civil sanctions, but still raise concerns in terms of civility and respect for others, States should focus on addressing root causes—including intolerance, racism and bigotry by implementing strategies of prevention—and adopting counter-narrative strategies.

- In terms of the different forms that State regulations concerning access to online content may take:
  - States are required to avoid the use of communications "kill switches" to shut down entire parts of a network or service.
  - States are required to ensure that the use of blocking or filtering techniques are established in law, justified to pursue a legitimate aim, a necessary and proportionate means to achieve the purported aim, including by being sufficiently targeted so as not to render a wide range of content inaccessible beyond that which has been deemed illegal, and subject to the intervention of or possibility for review by a judicial or independent body.
  - States are required to ensure that they never delegate censorship measures to private intermediaries, never hold them liable for refusing to take action that infringes the human rights of individuals, and never hold them liable for any third-party content unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to

remove it and they have the technical capacity to do that.

– States are required to ensure that any requests submitted to intermediaries to prevent access to content should be conducted through an order issued by a court or a competent body that is independent of any political, commercial or other unwarranted influences.

- States should ensure that individuals possess the necessary digital literacy necessary to make full use of the Internet, drawing particular guidance from the best practices identified within the recent reports published by the Global Commission on Internet Governance, the United Nations Special Rapporteur on Freedom of Expression, and the World Bank.

F. Access to Internet infrastructure

- States have a positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, which includes the Internet. As such, States should take all necessary steps to foster the independence of the Internet and to ensure access of individuals to it.
- Each State should develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of the population.
- Drawing particular guidance from the recent reports published by the Global Commission on Internet Governance, the United Nations Special Rapporteur on Freedom of Expression, the United Nations High Commissioner for Human Rights, and the World Bank, States should:

- Adopt measures to encourage competition and foster investment in networks;
- Facilitate network sharing;
- Invest in public access points;
- Ensure their taxation policies do not bias the market for Internet services or related equipment;
- Adopt policies to foster competition among the producers and sellers of Internet devices;
- Respect network neutrality by prohibiting attempts to assign priority to certain types of Internet content or applications over others for payment or other commercial benefit;
- Adopt policies to bridge the gender digital divide by ensuring that information and communications technologies are accessible to women on an equal basis without discrimination and promoting women's equal, effective and meaningful participation online; and
- Honour their commitment to facilitate technology transfer to developing States and to integrate effective programmes to facilitate universal access to the Internet in their development and assistance policies.

102. Two important issues pertinent to the relationship between human rights and ICTs are beyond the scope of this Commentary. Going forward, these issues will also require further attention and reflection by States, industry actors, civil society and academia.

103. First, in accordance with the human rights norm proposed in the GGE 2015 Report, this Commentary has focused on the responsibilities of States to respect and protect human rights in ensuring the secure use of ICTs. As such, the Commentary has omitted any articulation of the responsibilities of private actors in respecting human rights online. As already noted earlier in this Commentary, the private sector invests in, maintains and in

many cases owns vast social media forums, the infrastructure for mobile technology, the tools used by law enforcement and intelligence for surveillance and data-processing, and the devices or services on which most personal data is stored. As such, an examination of the private sector's human rights responsibilities should be a priority for the international community.[258]

104. Second, this Commentary has focused on the applicability of human rights online during times of peace, omitting analysis of the application of human rights obligations during times of armed conflict. According to the International Group of Experts within the *Tallinn Manual 2.0* process, "both the law of armed conflict and international human rights apply to cyber-related activities in the context of an armed conflict, subject to the application of the principle of *lex specialis*".[259] Equally, however, "[t]he precise interplay between the law of armed conflict […] and international human rights law remains unsettled and is determined with respect to the specific rules in question".[260] As such, clarifying this interplay in the cyber context should also be a priority for the international community going forward.

---

[258] See generally, Global Network Initiative, *Principles on Freedom of Expression and Privacy* (October, 2008); Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, in 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Entities', A/HRC/17/31, 21 March 2011; Telecommunications Industry Dialogue on Freedom of Expression and Privacy, *Guiding Principles* (March 2013); A/HRC/32/38; A/HRC/35/2; and Article 19, *Getting Connected: Freedom of Expression, Telcos and ISPs,* Policy Brief, June 2017.

[259] See, in this regard, Michael N. Schmitt (ed.), op. cit., page 181.

[260] Ibid.

Recommendation 13 (f)

A State 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.

Jason Jolley

Contextualization

1. The concern for the protection of national critical infrastructure against malicious and hostile cyber activities has been a crosscutting theme in the United Nations First Committee process, discussions of the Global Culture of Cybersecurity, as well as national cybersecurity strategies during the past two decades.[1]

2. The 2010 and 2013 GGE reports noted the growing use of ICTs in critical infrastructures and industrial control systems.[2] In 2015, the GGE held that "the most harmful attacks using ICTs include those targeted against the critical infrastructure". Furthermore, as ICT technology expands and states rely upon

[1] Ths chapter does not go extensively into discussion of the concept of critical infrastructure. See further, recommendations (g) and (h).

[2] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 30 July 2010 (A/65/201), para. 9; *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98), para. 9.

ICT technology to a greater extent, the strategic importance of ICT technology on a state's critical infrastructure will continue to grow. This strategic importance on behalf of the state increases the likelihood for retaliation and potential kinetic overflow from any interference on a states' ICT technology and infrastructure. The critical importance that ICT operations and a state's critical infrastructure play in developing societies cannot be understated. States continue to view their critical infrastructure as a strategic asset and retaliate against any act that impact their critical infrastructure. This may fuel an escalating continuum that may spill into the physical realm and threatens the peace and security of all states. By preventing states from utilizing ICT to the detriment of other states, recommendation (f) seeks to remove one more possible point of conflict between states.

3. Defining or otherwise conceptualizing critical infrastructure remains beyond the immediate focus of the group. There is no universally accepted definition or criteria of what constitutes critical infrastructure (CI). The term lends itself to several possible interpretations and approaches—CI can refer to critical objects, services, functions and sectors.

4. In this context, the Group has included, in their recommendations for voluntary and non-binding norms, a recommendation whereby States are called to abstain from damaging critical infrastructure that provides services to the public. Recommendation (f) elucidates a common-sense rule that embodies the ideas that serve as the baseline for the United Nations Charter, those being the maintenance of peace and security, taking effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.[3]

[3] United Nations, Charter of the United Nations, 24 October 1945 (1 UNTS XVI), Art 1(1).

5. The Group has based its call for CI protection on the concept of state responsibility. As in several other cases, the GGE therefore has included in the voluntary and non-binding norms section a concept that is otherwise considered legally binding. The GGE itself has emphasized the legal concept of state responsibility in the international law section of the report, concluding "States must meet their international obligations regarding internationally wrongful acts attributable to them under international law"[4] and "States must not use proxies to commit internationally wrongful acts using ICTs".[5]

6. To further facilitate CI protection, the GGE also draws attention to the need to provide assistance and training to developing countries to improve security of critical infrastructure[6] and facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders.[7] Furthermore, Experts stress the importance of development of mechanisms and processes for bilateral, sub-regional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure.[8]

Background

7. As noted, the recommendation that the GGE offers in support of critical infrastructure protection uses the basic construct of the law of state responsibility. One can only speculate why Experts have offered as voluntary something that by the majority of states is considered legally binding.

8. Those who consider the law of state responsibility legally binding refer to Draft Articles on Responsibility of States for Internationally Wrongful Acts (Draft Articles), a codification

---

[4] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174), para. 28 (f)

[5] A/70/174, para. 28 (e).

[6] A/70/174, para. 21 (b).

[7] A/70/174, para. 21 (e).

[8] A/70/174, para. 16 (d) i.

of the International Law Commission (ILC), as reflective of customary international law. Having taken almost four decades to codify, the rules of the Draft Articles have since been endorsed by the General Assembly and are considered highly authoritative.[9]

9. Consequently, one explanation can be that not all Experts agreed to the legally binding nature of the law of state responsibility. After all, as can be observed in national positions vis-à-vis the work of the International Law Commission, there are different views as to the legal status of the Draft Articles.[10] It may be, as Adamson notes above, that Experts' move to use the language of state responsibility may have to do with the fact that the Group has wanted to re-define or re-emphasize (parts of) it strictly in the context of state uses of ICTs. The rest of this commentary is based on the standpoint that the law of state responsibility as the basic construct of recommendation (f) is binding upon states.

10. The law of state responsibility can broadly be explained by its two underlying principles: states can be held responsible for acts that are attributable to them and states can only be held responsible for internationally wrongful acts, that is, for breaches of their obligations towards other states.

11. A state may owe an obligation "to another state, several states, or the international community".[11] These obligations may be specific, arising from treaty obligations a state may have with another state, or more general, as those arising from customary international law. A state's treaty obligations will bind only those signatories to a specific treaty, while customary international law will bind all states, unless those states have specifically objected to the formation of the custom, and even

---

[9] Jan Klabbers, *International Law* (2nd ed. 2017).

[10] *See,* Michael N. Schmitt (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0* (Cambridge University Press, 2016), para. 3-5.

[11] *Draft Articles on the Responsibility of States for Internationally Wrongful Acts, art. 33*, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

then, a state may be bound by customary international law.[12] In respect to ICT obligations, a state's obligations derive mainly from customary international law as there is limited treaties in place regarding ICT operations.[13]

12. Recommendation (f) addresses a state's obligations regarding ICT operations undertaken by the state. It reaffirms the rule that if a state owes an obligation under international law in the kinetic realm, it owes the same obligation in respect to the cyber realm and ICT operations.[14] A state under international law may be responsible for any violation of its international obligations irrespective of the domain in which the violation occurs. Recommendation (f) expands upon the state's customary obligation by imposing a prohibition upon a state for conducting or "knowingly support[ing]" ICT activities, which would violate a state's obligations. This idea, while simple on its face, requires a discussion on the customary international law of state responsibility to further unpack the application of this rule. This will be addressed below.

13. The discussion herein is provided in a doctrinal manner to allow states, commentators, and interested parties a means to assess the validity of the discussion and the norms presented without engaging in in-depth political and legal theory. The author believes that it is important in this space to present the needed information in such a manner as to allow all states, irrespective of legal, social, and political systems, a tool for understanding and applying the norms presented herein.

14. In addition, the international law discussed herein is presented *lex lata*, while the field of international cybersecurity law and the law of ICT operations are evolving and growing. Any discussion must be based on existing international law so as to be a valid means of implementing the norms presented. This style has been adopted to ensure a shared understanding across cultures, legal systems, and ideologies as it is believed

---

[12] Roozbah B. Baker, *Customary International Law in the 21st Century: Old Challenges and New Debates,* (21 Eur. J. Int'l L. 173, 2010).

[13] Michael N. Schmitt (ed.), op. cit.

[14] Michael N. Schmitt (ed.), op. cit.

that without a shared understanding of the ideas discussed, each state may implement the ideas presented herein in a disparate manner not necessarily in harmony with other states, which may lead to misunderstandings further down the road as it were.

15. Recommendation (f) simply applies a state's existing international obligations to each state's ICT activity. A state per recommendation (f) only need apply its existing obligations to ICT operations.

16. For simplicity sake, the rest of this commentary will break recommendation (f) into its constitutive elements and discuss each standing alone. While each element contained within the recommendation is dependent upon the all the elements contained within recommendation (f) and read as such, each element standing alone must be met for the norm to apply. The analysis will begin with a discussion on the concepts contained within the element that "[a] State should not conduct or knowingly support…" It will further elaborate on the legal obligations a state may have in regard to ICT obligations, and general state obligations contained within the phrase "ICT activity contrary to its obligations under international law…" It continues by addressing the element of "intentionally damages critical infrastructure…" and the ideas contained within "or otherwise impairs the use and operation of critical infrastructure to provide services to the public." The final part of this commentary will discuss recommendation (f) as a single idea and bring the constitutive elements into focus as a single prohibition on state conduct. The section will conclude with a focus on why it is in the state's best interest to adopt the rules presented herein.

Expansion and analysis

A State should not conduct or knowingly support

17. The state is the basic actor in international law, a state does not exist, however, without the individual agents that enable the state to act. The state is a collection of individual agents working in furtherance of the state's aims. In turn, the

state as an entity is responsible for the acts of these individual agents in international law, within the defined parameters of the law of state responsibility. For the purposes of this commentary, it is enough to understand that the state will be responsible for any conduct that amounts to an international wrongful act attributable to it. Simply put, if a state violates its obligation in respect to another state or states, it has most likely committed an internationally wrongful act. If that wrongful act is attributed to the state, then the state is responsible under international law.

18. Here, then when we discuss the state, it should be understood that we are discussing the acts of the agents of the state for which the state bears responsibility. There are exceptions to this general rule, particularly when a state is responsible for the acts of non-state actors, which will be addressed below when this commentary discusses the issue of "knowingly allow[ing]."

19. The use of the phrase "should not" as used within this element is simply a articulation that a state not engage in behaviour that violates its international obligations and that states not engage in activity discussed in recommendation (f) and should be understood and read in context with the norm *in toto*. Like other obligations discussed below, it is not an absolute obligation but an obligation that is subject to a state's other obligations, e.g., a state may under some circumstances find it necessary to target critical infrastructure but such acts would have to comply with existing International Humanitarian Law, United Nations Charter art. 2(4) and art. 51 and such response would have to be necessary, proportionate, and the target distinct. This will be explored briefly below.

20. Conduct, to borrow a concept from criminal law, is simply the *actus reus,* that is, the act itself of engaging in ICT activity that violates the prohibition contained within recommendation (f). Unlike the issue of knowingly supporting, a breach of international obligation requires no intent on behalf of the state itself. Therefore, recommendation (f) places a blanket prohibition on any act on behalf of the state for any violation the state itself undertakes that would violate the

prohibitions falling within the scope of the recommendation with limited exceptions.

21. The prohibition of breach of an international obligation may be violated in extreme circumstances, as discussed above. A state may, in extreme cases, find it necessary to violate its obligation and, in the context of recommendation (f), intentionally damage or impair critical infrastructure. It is hypothesized that such incidents may be extremely rare, but it is not beyond the realm of reason to believe that a state may be targeted by another state conducting ICT operations via that state's critical infrastructure. In such a case, where a state is utilizing its own critical infrastructure to target another state, and the harm resulting from such an act is of such magnitude as to justify violating this recommendation, then a state out of necessity may target the critical infrastructure of the attacking state, if the attack on the critical infrastructure is proportional to the prevented harm. Such an act though on behalf of the attacked state may not be a generalized attack upon the critical infrastructure. Such an attack must be distinct enough to target the specific infrastructure involved and not damage any other infrastructure beyond that which is necessary to stop the attack.

22. Knowingly supporting acts which may violate recommendation (f) is a more complex idea. Knowledge may be direct or indirect and encompasses the specific intent to support acts in violation of the norm in discussion. *Supporting* as used herein may refer to the issue of states utilizing proxies or hacktivists or other non-state actors to violate its international obligations without actually accruing international responsibility for those acts. *Knowing* also implies an intent on behalf of the state, which is separate but aligned idea within the knowledge prong. For the purposes of this commentary, knowledge is two concepts, the knowledge that the support in question will result in the violation of the obligation, and the state intends to violate it. This commentary will separate out these distinct issues, the issue of knowledge, the intent element, and the issue of support to demonstrate how these issues apply in the context of recommendation (f).

23. Knowledge may be understood as "[a]n awareness or understanding of a fact or circumstance."[15] Knowledge by a state in the context of recommendation (f), would be knowledge that the state has direct and clear knowledge of a fact derived from its own agents or from other sources.[16] This direct knowledge may concern an act on the behalf of a state or an omission,[17] that is, a state may have direct knowledge of an act on its own behalf or that of another. An omission, would occur when a state has direct knowledge of an act that would violate an obligation, within its jurisdiction that it passively supports, but takes no action to prevent or stop. Both of these, the act or the failure to act (omission) would violate the prohibition on conduct put forth in this recommendation.

24. Knowledge may also be indirect, either constructive or imputed. Constructive knowledge is "knowledge that one using reasonable care and diligence should have, and therefore is attributed by law to a given person [or State]."[18] Constructive knowledge is important as a state is expected to use due diligence to ensure that its territory is not used to the detriment of another state.[19] This knowledge however is impacted by the state's technical ability to monitor and control its networks and will vary by state. A state may be responsible for the breach of an obligation if the state has constructive knowledge that an ICT operation that, in the context of recommendation (f), targets CI is being conducted from its territory and does not, within its technical abilities, attempt to prevent such act from occurring, thus having both constructive knowledge and passively supporting the ICT act by the state's lack of action.

25. Imputed knowledge is an important concept giving the growing issue of state's utilizing non-state actors (proxies/

---

[15] Black's Law Dictionary (2011).

[16] Ibid.

[17] *Draft Articles on the Responsibility of States for Internationally Wrongful Acts, arts. 4-11* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

[18] Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9).

[19] *See generally,* ibid.

so-called hacktivists) to engage in activities, which, if conducted by the state, would result in responsibility. But, to avoid international responsibility, states may engage non-state actors to initiate the unlawful act without oversight or control by the state. Imputed knowledge (also called implied knowledge) is "knowledge attributed to a given person [or State]"[20] based upon the relationship of the parties. If an agent of a state has knowledge of ICT activity contrary to an obligation of that state, that knowledge may be imputed to the state itself, just as if the state had direct knowledge. Applied to recommendation (f), imputed knowledge would implicate the state if a state agent, subject to the laws of international responsibility, engaged a non-state actor to carry out ICT activity that would violate the obligation. This issue of engaging non-state actors will be explored below.

26. Finally, with respect to *knowingly*, the language of recommendation (f) allows concluding that the state must act with intent to support activity that would violate the obligation. That is, in addition to having knowledge that the activity would violate the obligation, the state must act with specific intent (or to borrow from criminal law *mens rea*) in supporting activity that would violate the prohibition. If a state inadvertently supports an activity that violates the prohibition contained within recommendation (f), then the state has not violated this norm. The state must actively and with specific intent support activities that violate the obligation to be in violation.

27. The term *support* may be understood as assistance, normally in the form of monetary or technical assistance.[21] Recommendation (f) fails to specify whom the state must knowingly support and fails to elucidate a standard of support that a state must meet in order for it to violate it. The GGE specifically named "malicious non-State actors, including criminal groups and terrorists"[22] as existing and emerging threats. However, *support* should be understood to encompass

[20] Black's Law Dictionary (2011).
[21] "Support," Oxford English Dictionary (2017).
[22] A/70/174, para. 7.

all non-state actors. While the GGE is correct in identifying these as emerging threats, any support of individual non-state actors irrespective of their role would result in a violation in the meaning of recommendation (f).

28. The more complex question, is to what level a state must support a non-state actor in order for the state to violate its international obligations. While any knowing support on behalf of a state may trigger a violation, a state does not violate its international obligations and incur international responsibility without a much greater showing of support. The International Court of Justice, when discussing at what level the United States support for Nicaraguan Contras during the Nicaragua Civil War (1980-1986)[23] invoked international responsibility for the acts of the Contras to the United States, found that the United States had provided logistical support, monetary support, training, intelligence support, identified targets, and advised the Contras on all aspects of military operations, yet despite this support the United States was not responsible for the acts of the Contras and had not violated its international obligations.

29. It must be understood therefore that for a state to violate its international obligations by supporting non-state actors the support on behalf of the state must be substantial and verging on the point where there is virtually no difference between the support shown for the non-state actor and the support that the state would give its own agents or internal bodies. It must be noted though that this rule is controversial and its application to ICT activities is much debated. For the purposes of this commentary, until further custom develops in regard to ICT activities and non-state actors, the support must be substantial for the state to violate its international obligations to incur international responsibility.

Acting contrary to a State's obligations and ICT operations

30. A state's obligations in international law derive from the state's individual treaties in place and customary international

[23] Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.) (Merits), 1986 I.C.J. Rep. 14.

law. As such, a state has numerous obligations that may impact its obligations in regard to ICT operations. As it is impossible to identify and discuss each potential obligation, this commentary will briefly discuss those obligations, which arise from both treaty law and customary international law that a state may violate by their ICT operations. The obligations discussed derive from the Charter of the United Nations, the Universal Declaration of Human Rights, and International Humanitarian Law. In addition, this commentary will briefly discuss the concept of *jus cogens* norms.

31. The United Nations Charter imposes obligations upon all states as the United Nations Charter is the supreme treaty law that binds all states. The primary purpose of the United Nations Charter is to ensure "international peace and security"[24]. To that end the United Nations Charter prohibits states from utilizing the threat or use of force by states except in self-defence. The United Nations Charter art. 2(4) declares that "[a]ll [m]embers shall refrain in their international relations from the *threat or use of force against the territorial integrity or political independence of any state*, or in any other manner inconsistent with the Purposes of the United Nations."[25] This obligation, the prohibition on the use of force, is considered a peremptory norm in international law, that is, it is an obligation imposed upon a state that may not be derogated from.[26]

32. The obligation contained in art. 2(4), may be violated, intentionally or unintentionally, in ICT operations. Where a state initiates an ICT operation on another state with the intent for that operation to harm a specific target, if that ICT operation reaches the legal threshold of force, and if the operation is not in self-defence,[27] then the state initiating the operation has violated article 2 (4) as well as the prohibition contained in recommendation (f), provided that the operation "intentionally damages critical infrastructure or otherwise impairs the use and

---

[24] United Nations Charter, Art. 1(1) (1949).
[25] United Nations Charter, Art. 2(4) (1949). (Emphasis added).
[26] Ian Brownlie, *Principles of Public International Law* (5th ed., 1998).
[27] See, United Nations Charter, Art. 51 (1949).

operation of critical infrastructure…". Simply put, if a state launches an operation via the ICT domain and that operation intentionally damages or impairs critical infrastructure, then it meets the elements of prohibition contained in recommendation (f). A state may also unintentionally violate art. 2(4) if it initiates an operation that unintentionally results in damage that would be considered to be the equivalent of the use of force.[28] Such use of the ICT domain to conduct a use of force will be also governed by the rules of International Humanitarian Law discussed below.

33. The prohibition set forth in recommendation (f) will also be violated if a state knowingly supports a non-state actor who engages in ICT operations against another state, if those non-state operations result in intentional damage to critical infrastructure or otherwise impairs. As discussed above however, implementation of recommendation (f) is subject to the customary international law of state responsibility for the assignation of responsibility for the acts of non-state actors. It is important to note that, as ICT operations and cyberspace mature, these rules will likely change. The rules applied by this commentary are the current international law, but as the applicable laws in place are based upon physical acts and not per se ICT operations, it is reasonable to believe that the existing laws of state responsibility and other applicable international law will evolve and become specific to the ICT environment.

34. International Humanitarian Law (IHL, also Law of Armed Conflict/Law of War)[29] is the international law that governs the use of force between states. IHL is concerned with the protection of non-combatants and regulates how states may engage in

---

[28] What constitutes force in international law in respect to ICT operations is not settled law. For the purposes of this commentary force should be understood as the equivalent of an attack resulting in the loss or damage of either physical infrastructure components or the loss of software and data controlling those components thus resulting in an operational loss of critical infrastructure on par with the physical destruction of the infrastructure on equal to or exceeding the damage that would have been caused by a kinetic weapon attack.

[29] International Committee of the Red Cross, *What Is International Humanitarian Law* (2004).

conflict. IHL does not govern when states may use force, just how the force is utilized.[30] IHL is derived from both treaty law (Geneva Conventions of 1949, the Additional Protocols to the Geneva Convention of 1977, and other international accords) and customary international law. IHL arguably governs the conduct of hostilities by all states, even non-signatories to the treaties, due to the belief that the treaties that form the bulk of IHL have become part of the customary international law, which binds all states.

35. The principles of necessity, proportionality, and distinction briefly discussed above are some of the legal principles found in IHL. For instance, IHL Rules 11-13[31] discuss the prohibition against indiscriminate attacks. Rule 12 defines indiscriminate attacks as those attacks:

- Which are not directed at a specific military objective;
- Which employ a method or means of combat which cannot be directed at a specific military objective; or
- Which employ a method or means of combat the effects of which cannot be limited as required by international humanitarian law; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

36. Any ICT operation that violates the obligation of distinction, which impacts a state's critical infrastructure as put forth in recommendation (f), would violate the prohibition contained therein. The second and third criteria above are particularly relevant to the discussion herein; for instance, if a state utilizes malicious software that is indiscriminate in its attack and does not distinguish between a specific military target or the effects of the malicious software go beyond the target and damages or impairs critical infrastructure, then a

[30] Ibid.

[31] International Committee of the Red Cross, IHL Database, Customary IHL, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule11 (2017).

state has violated its obligation against indiscriminate attacks and violated the state's obligation under IHL and violated its international obligations in the context of recommendation (f).

37. The rules of proportionality and necessity may also impact the obligations discussed herein. IHL Rule 14 holds that "[l]aunching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited".[32]

38. Rule 14 also holds that any military operations that potentially impact civilian objects such as critical infrastructure must confer a military advantage to the military attacking the target. This, combined with the rule that the attack must be a military necessity, the effects of the attack must be balanced against potential harm of civilian population or object. Again, if a state violates the obligation contained within Rule 14, and the violation intentionally targeted civilian infrastructure resulting in intentional damage thereto, or otherwise impairs the use of critical infrastructure, then the prohibition proposed in recommendation (f) has been violated.

39. IHL is particularly germane to the issue of targeting civilian infrastructure either intentionally or unintentionally as military and civilian ICT infrastructure in cyberspace is significantly intertwined and it is almost impossible to separate the two out for the purposes of attack. The IHL rule of distinction is such as an attacking party utilizing the ICT domain is virtually certain to violate the prohibition aspired in recommendation (f) either intentionally or unintentionally if they seek to damage an opponent's infrastructure via ICT operations. A prime example of this is the Stuxnet virus, which was launched against Iranian nuclear centrifuges in a targeted attack, which, in this author's reading, violated art. 2(4) as discussed above, and also incidentally interfered with other SCADA controllers not associated with the Iranian nuclear program, thus violating the rule on distinction. Even though that

[32] Ibid., page 32.

malware was specifically designed for the targets in Iran, the spread of the virus to other civilian targets violated the state's obligation on distinction in military operations and thereby constituted both an illegal use of force, and a violation of IHL.

40. IHL imposes numerous obligations and prohibitions on states who attempt to utilize the ICT domain for military purposes. IHL protects civilians and civilian infrastructure and places a heavy burden on states to avoid targeting civilian targets without an overwhelming military need, and limiting any attack to the smallest attack needed to reach the military objective. IHL protects non-combatants and combatants that have left the conflict, medical and religious personnel and infrastructure, journalists, cultural artifacts, and the natural environment and more. Hence any violation of these obligations to protect these specific person and objects that intentionally damage or otherwise impair critical infrastructure would violate the prohibition sought in recommendation (f).

41. Customary International Law (CIL) may impose obligations upon specific states (localized or regional custom) or all states. CIL arises from state practice, and the idea that the state is bound to that practice out of a sense of legal obligation (*opinio juris*). CIL may result from general practice, such as coastal fishing, or as a result of a specific stimuli, such as the acts of the United Nations General Assembly.[33] There is no specific timescale for the formation of CIL and no notice requirement to states. Once CIL arises, states are presumed to know about the obligations imposed by the custom. For the purposes of this commentary, it is important to understand that the CIL may impose obligations upon states that when violated may violate requisite elements contained in recommendation (f). It is important to note that a state may not be aware of its international obligation in respect to its CIL obligation and yet still violate it.

[33] Bin Cheng, *United Nations Resolutions on Outer Space: "Instant" International Customary Law?* (5 Indian Journal of International Law 23, 1965).

42. An example of a CIL rule that states may violate is the CIL rule that it is "every state's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states", derived from the *Corfu Channel* Case.[34] Generally speaking, a state may not allow its sovereign territory to be utilized to cause harm to another state. If a state knowingly allows its territory to be used to cause harm another state, for example, through environmental harm caused by industry, allowing bases for terrorists, or allowing non-state actors to utilize its territory to utilize its ICT infrastructure to conduct malicious acts, etc., then that state has violated its obligation under this CIL rule, and if that violation results in intentional damage or interference with a state's infrastructure then the obligation in recommendation (f) has been violated.[35]

43. It is important to note that, in addition to the specific obligations discussed and the general CIL obligations, there are numerous other treaties that a state owes obligations under. A state owes obligations under the human rights treaty, the genocide convention, multiple terrorism convention, environmental conventions, undersea telegraph conventions, etc. Any violation of an obligation owed under any international convention or CIL in addition to meeting the other elements discussed in recommendation (f) will result in a violation. A state owes a duty to meet its obligations and ensure that it does not violate intentionally or not its international obligations.

44. Finally, it is important to remember that specific legal regimes in international law may be controlled by specialized legal regimes (*lex specialis)*. These specialized regimes may impact the legal aspects of ICT operations and will be discussed briefly to ensure proper information exchange.

---

[34] Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9). For a brief discussion on the case, *see*, Michael N. Schmitt, Pre*emptive Strategies In International Law* (24 Mich. J. Int'l L. 515, 523 2003).

[35] For further discussion of the legal concept of due diligence, see, commentary to recommendation (c).

45. The customary international law of state responsibility applies to the issues involved with attribution and state responsibility of ICT operations.[36] However, there is debate as to whether the customary international law of state responsibility has been altered in its application to ICT activities in regard to attribution and state responsibility. Recent state practice has demonstrated that many states use an altered method of attributing ICT activity in cyberspace that do not necessarily meet the criteria for attribution set forth in the *Draft Articles*.[37] This altered method of attribution for the purposes of state responsibility may constitute a self-contained regime within international law.

46. The idea of self-contained regimes within international law itself is a contentious issue with many commentators debating whether or not self-contained regimes exist in international law.[38] This commentary takes no side in the debate, the discussion is presented to allow individual readers to understand the issue for themselves. However, the debate concerning ICT activity as a self-contained regime is bolstered by the fact that many states utilize ICT activities to the detriment of other states in peacetime and the CIL of ICT activity is arguably evolving in regard to peacetime ICT operations.

47. If the law governing ICT activity is a self-contained regime with specialized rules for attribution and state responsibility, then the law governing ICT activity would be considered *lex specialis*.[39] This designation as *lex specialis* is important as the law of ICT activity and its specialised rules of attribution and state responsibility would take precedent over the general rules of state responsibility. While this is an evolving issue without

---

[36] Michael N. Schmitt (ed.), op. cit.

[37] *Draft Articles on the Responsibility of States for Internationally Wrongful Acts, arts. 4-11* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001)

[38] Michael N. Schmitt (ed.), op. cit.

[39] *See*, Dorota Marianna Banaszewska, *Lex Specialis* (Max Planck Encyclopedia of Public International Law, 2015).

a clear agreement by commentators, the idea that the law governing ICT activity as *lex speciais* is an important one.

48. If the law governing ICT activity is *lex specialis*, then the specialised rules concerning ICT activity will take precedent over general rules of CIL and would allow states a means to address the nuances involved with governing ICT and address the challenges of attributing malicious ICT activity which challenges the existing rules of state responsibility and attribution. This, however, is not a settled issue and will continue to be a contentious issue with international law commentators. It is important to be cognizant of the issue though as it will continue to influence the debate and evolution of the law governing ICT activities.

Intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public

49. The final part, for the purposes of our discussion on recommendation (f), deals with the final two elements dealing with intentionally damaging or otherwise impairing critical infrastructure. While this last part of recommendation (f) may be read as two distinct elements, for the purposes of this commentary, they will be discussed together, as both elements deal with the result of the state's ICT conduct.

50. The discussed element contains two prohibitions on states. A state may not intentionally damage critical infrastructure and a state may not otherwise impair the use and operation of critical infrastructure to provide service to the public. These prohibitions relate to the result of a state violating its international obligations and rely upon whether the state conducted or knowingly supported violations of its international obligations, which resulted in intentional damage or otherwise impaired critical infrastructure. These two distinct ideas encompass the specific intent prohibition on intentionally damaging and a strict liability (that is responsibility without the intent to damage or in this case impair) on a state for its ICT operations that impair critical infrastructure without the specific intent to do so. Before delving into the details of each of these

ideas, it must be understood that the specific intent element (intentionally) applies to the issue of "critical infrastructure" while the strict liability element applies to the resulting harm which must impair "the use and operation of critical infrastructure to provide services to the public.

51. The specific intent element holds that a state must intentionally be (conducting or knowingly supporting) violating its international obligations and intentionally damaging the victim state's infrastructure for a violation to occur within the meaning of recommendation (f). If a state unintentionally damages a state's infrastructure, and as long as the unintentional violation does not impair the use or operation of critical infrastructure that provides services to the public, then no violation occurs. This specific intent, intentionally, should be understood to mean an act that is deliberate or with specific purpose.[40] In this instance, if the state utilizing ICT to damage another state's critical infrastructure does so deliberately, knowing that its acts will most likely result in damage to the victim state's critical infrastructure, then the prohibition aspired by recommendation (f) is violated. For this prohibition to be violated, there must be the deliberate act and damage to critical infrastructure. The level of damage in this element is not important for the purposes of the discussed recommendation, it is enough that the victim state suffers damage.

52. If the state utilizing ICT unintentionally damages another state's critical infrastructure providing services to the public and that critical infrastructure is impaired, then a violation of the prohibition contained in recommendation (f) has occurred. The intent of the state utilizing ICT as a vector is not important in this instance; the violation is based simply on the fact that a state's ICT operations impaired another state's public critical infrastructure, which provided services to the public. There is no need to show any intent on behalf of the state utilizing ICT. The wrongfulness of the act rests solely on the act itself, that is the impairing of public critical infrastructure.

---

[40] Oxford English Dictionary (2017).

53. *Impair*, for the usage of recommendation (f), should be understood as any damage, physical or electronic, including the loss of data or software, or interruption of digital services provided by critical infrastructure, that makes the critical infrastructure less effective, less valuable, operate worse, or inhibit use by the public, the threshold being that the public must be impacted, even minimally. The issue of providing public services in general, should be understood as applying to any service provided to the public, as long as that service provided is part of a state's critical infrastructure.

54. As discussed above, a state must be cognizant that, due to the technology supporting the ICT infrastructure, separating legitimate military CI and civilian CI that provides a service to the public may be impossible. Thus, any impairment, irrespective of the ICT target or intent of the state utilizing ICT as a vector will trigger a violation of the prohibition contained in recommendation (f).

Recommendations

- Recommendation (f) specifically engages states not to act either intentionally or unintentionally in any manner via ICT that would impact the critical infrastructure that the public may rely upon. By implementing recommendation (f), states may effectively reduce attacks against critical infrastructure and thereby strengthen international peace and security, including stability.
- It must be reiterated again that recommendation (f) does not introduce any new obligations upon any state. If anything, it echoes, for instance, the rules set forth in IHL concerning the protection afforded to civilians and non-combatants. Implementation of this recommendation, consequently, is based upon a state's existing international obligations. This makes recommendation (f) particularly important as it holds states accountable for violating existing obligations and applying those obligations to the ICT realm. It is therefore recommended that states

endorse and accept this recommendation, and other recommendations reflecting or building upon already established international law, in the spirit of the GGE 2013 conclusion that "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".[41]

- Furthermore, it is in the best interest of states to voluntarily adopt the GGE recommendations. The GGE recommendations essentially give states a roadmap for their activities in regard to ICT.[42] The GGE roadmap, as it were, strengthens the probability that conflict will not happen as a result of ICT activity, a real possibility without the adoption of the GGE recommendations.

[41] A/68/98, para. 16.

[42] See also, Tikk and Kerttunen The Alleged Demise of the United Nations GGE: An Autopsy and Eulogy (2017).

Recommendations 13 (g) and (h)

States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

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.

Michael Berk*

Contextualization

1. The concerns over securing global information and telecommunications systems and infrastructure from malicious attacks, including terrorism, evolved along with the continued development of ICTs throughout the 1990s.[1] The

* Visiting Research Fellow, Center for Cyber Security an International Relations Studies, University of Florence. Member of the OSCE Academic Steering Group on confidence building measures in cyberspace and President of Alton Corp., a security consulting firm.

[1] See, for instance, *Role of science and technology in the context of security, disarmament and other related fields*, Report 53/576 of the First Committee of 18 November 1998), A/63/576.

growing recognition that ICTs can contribute to the beneficial development of the entire international community was on the other hand offset by concerns that these technologies "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States."[2]

2. Following the 1998 recommendation by the United Nations First Committee, subsequent resolutions by the United Nations General Assembly between 1999 and 2010 based on country submissions and continued international dialogue demonstrate an evolving understanding of and concerns for the integrity and availability of uninterrupted provision of information networks and services. Throughout these resolutions, specific attention was given to potential threats of misuse of ICTs by terrorist and criminal groups. Over time, serious concerns emerged also over state-to-state conflicts involving ICTs and the possibility of disrupting an adversary's critical information and/or other national infrastructures through malware or third parties.

3. The first United Nations GGE in 2003-2004 did not result in a consensus report. In the 2009-2010 they did, with the 2010 report stating that while there were "few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs", their use of ICT for internal communication and organization, recruitment, financing and promotion of extremist and terrorist ideas and actions presents a significant concern. At the same time, it was noted, "the growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption".[3] Due to the continued expansion of ICTs globally and the rise of associated incident levels involving civilian and military infrastructure, these concerns have been repeatedly voiced in the subsequent

---

[2] *Developments in the field of information and telecommunications in the context of international security*, Resolution 53/70 of 4 December 1998 (A/RES/53/70).

[3] Report of the "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations GA, A/65/201 (30 July 2010), para. 6 and 9.

United Nations GGE reports from 2013[4] and 2015.[5] The increasing deployment of ICTs in industrial control systems and across many civilian sectors and infrastructures, such as banking, transportation, energy production and electric grid systems exposed new dependencies and expanded the potential list of targets. In 2015, the rising levels of attacks against these installations and associated information systems of a State caused the GGE to call them "the most harmful", pointing out that the risk is "both real and serious". While noting a "dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors" the report for the first time specifically draw attention to the fact that many states began developing ICT capabilities for military purposes, which is likely to lead to their use in future conflicts.[6]

4. The concern for protecting critical information and national infrastructure against proliferating cyber threats guided the development of a number of GGE norms. Specifically, while recommendation (f) ("not to support intentional damage"), recommendation (g) ("take appropriate measures to protect") and recommendation (h) ("respond to requests for assistance") directly address critical infrastructure protection (CIP) concerns and scenarios, three additional norms on the list covering related issues demonstrate a clear GGE intent to advocate for the establishment of a more comprehensive international normative framework for CIP. These norms include:

- Recommendation (i) ("integrity of the supply chain");
- Recommendation (j) ("responsible reporting on ICT vulnerabilities"); and
- Recommendation (k) ("not to harm information systems of emergency response teams").

---

[4] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98).

[5] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174).

[6] Ibid., para, 3-5.

Covering a wider range of potential state and non-state actors' behaviours, these latter recommendations provide prescriptive directions to states on technological, organizational and institutional matters to enhance the overall security of domestic and international CIP regimes.

5. Moving beyond the recommendations themselves, the GGE intent for the global normative framework on responsible state behaviours with regard to CIP is clearly exhibited in other parts of the GGE reports dealing with confidence- and capacity-building measures.

6. Thus, in the 2010 report, experts recommended a number of cooperative measures to further dialogue among states on norms pertaining to state use of ICTs to "create a global culture of cybersecurity", enhance mutual understanding of risks and information sharing between states, reduce collective risk and protect critical national and international infrastructure. Specific attention with regard to both enhancement of CIP and inter-state collaboration was given to capacity-building activities aimed at bridging the ICT divide between countries and enhancing national and international cybersecurity.[7]

7. In the 2013 report, the expert group, while reinforcing earlier assessments and recommendations made in 2010, focused on cooperative measures between States aimed at enhancing mutual understanding and responsible behaviour, including with regard to CIP. As such, it confirmed a number of recommendations, including, among others:

- "State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory";[8]
- "States must meet their international obligations regarding internationally wrongful acts attributable to them. States

[7] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 30 July 2010 (A/65/201), para. 12, 14 and 15, 18(i), and 17 respectively.

[8] A/68/98, para. 20.

should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs";[9] and

- "States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services".[10]

8. Furthermore, the report offered a number of recommendations focusing on confidence-building measures, including practical steps States could undertake to enhance mutual understanding and collaboration. While none of these specifically mentioned critical infrastructures, it goes without saying that the overall intent to increase cooperation, transparency and predictability between States on cyber-related issues, such as information sharing agreements dealing with best practices or incidents and inter-CERT collaboration, would also be conducive to the creation of bilateral and international frameworks for addressing cyber challenges related to critical infrastructure protection and handling of such incidents.

9. Also in the 2013 report, the GGE focused on capacity-building measures, including recommendations related to providing assistance for improving the security of critical ICT infrastructure, technical and other assistance to build capacity in ICT security in countries requiring such assistance and other activities aimed at raising cybersecurity culture and capabilities across all national sectors.[11]

10. Building on these foundations laid out in previous reports, the GGE report in 2015 expanded on confidence- and capacity-building recommendations with regard to CIP. In order to "enhance trust and cooperation and reduce the risk of conflict", the Group recommended that states consider among other CBMs the voluntary provision of "their national views on categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-

[9] A/68/98, para. 23.
[10] A/68/98, para. 24.
[11] A/68/98, para. 30, 31 and 32 (a-e).

enabled infrastructure". Moreover, states were recommended to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders".[12] Among the specific measures proposed were:

- "A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;
- The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;
- The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;
- The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents."[13]

11. In the paragraph that followed, experts suggested that an additional confidence-building measure with regard to CIP could be the strengthening of "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".[14]

12. The presented trajectory in evolution of international efforts starting in the 1990s and leading to the 2015 GGE report underlines the growing global realization that national and international risks associated with the globally interconnected ICT networks require cooperative and concerted responses.

[12] A/70/174, para. 16 (d)
[13] A/70/174, para. 16 (d) (i-iv).
[14] A/70/174, para. 17 (a).

Over the past two decades, United Nations member states have repeatedly affirmed the need for international cooperation against threats in the ICT sphere in order to combat the criminal and malicious misuse of information technologies, to create a global culture of cybersecurity and implement essential measures that can reduce risks to critical infrastructures.

Background

13. The evolution of GGE recommendations related to CIP is closely linked with the development of ICTs since the late 1990s. Faced with the potential, and later the reality, of technical disruption of normal functioning of critical infrastructures (CI) in ways that could have serious consequences to their economies and potentially result in loss of life, governments, corporations and the international community began discussions about developing and adopting CIP norms at national and international levels.

14. Following the successive United Nations General Assembly resolutions 55/63 in 2001 and 56/121 in 2002 on the need for states to enhance their efforts to combat cyber-crimes and misuse of ICTs, and to protect information systems, the 2003 United Nations General Assembly resolution 57/239 recognized that the responsibility for an effective cybersecurity "is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society".[15] The increasing penetration of ICTs into modern life and growing dependence of governments, businesses and individual users on them necessitated the adoption of the global culture of cybersecurity where all relevant state and other actors "must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies".[16] The resolution outlined nine complementary elements as normative

[15] *Creation of a Global Culture of Cybersecurity*, Resolution 57/239 of January 31 2003 (A/RES/57/239).

[16] Ibid.

recommendations that participants in national cybersecurity domains must address at their own levels of engagement and responsibility.

15. A more determined attention to the protection of critical infrastructures in the context of creating a global culture of cybersecurity manifested itself in the United Nations General Assembly resolution 58/199 on "Creation of a global culture of cybersecurity and the protection of critical information infrastructures".[17] Recognizing that the infrastructure-internet nexus has become a strategic vulnerability for most countries around the world and that disruptions in its regular operations pose numerous threats to their national security and, potentially, international peace and stability, the United Nations General Assembly put forth 11 elements aimed at protecting CIs. Among others, these elements outlined specific steps States and other relevant actors could adopt to protect CI through the establishment of effective national frameworks and modalities, increased international cooperation and information sharing, and provision of technical assistance to other states that require it for capacity building or in times of incident response and management.

16. Cyber-attacks against individual states (e.g., Estonia in 2007, Georgia in 2008, Myanmar in 2010) and critical infrastructures (e.g., Stuxnet used against Iran's nuclear facility), and the development and employment of military cyber capabilities sparked an urgent and intense debate about the importance of norms for state responsibility in cyberspace to ensure the safety and security of the internet and internet-based infrastructure. Many key organizations in the ICT community and beyond, including the International Telecommunications Union (ITU), G7/G20, ICANN, regional security organizations (such as NATO, OSCE, ASEAN and the Shanghai Cooperation Organization) and major, concerned and aspiring nations became vocal in this normative-political debate.

---

[17] *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, Resolution 58/199 of January 30, 2004 (A/RES/58/199).

17. Launched in 2007, the ITU's Global Cybersecurity Agenda focused on five pillars, including capacity building and international cooperation among them. As the facilitator for the successive World Summits on the Information Society (WSIS) from 2002 onwards, ITU was responsible for implementing activities in accordance with the WSIS action line 5, "building confidence and security in the use of ICTs", which included among others the development of the 2009 "ITU National Cybersecurity/CIIP Self-Assessment Tool".[18] The Tool offered ITU member states a comprehensive package of information, best practices and recommendations aimed at enhancing states' ability to protect their critical information infrastructure, creating a culture of national cybersecurity awareness and adopting measures that facilitate international collaboration.

18. As a primary transatlantic security organization comprising 57 participating states, including former Cold War adversaries, the OSCE demonstrated a growing degree of attention to issues surrounding cybersecurity of critical infrastructures over the years. For example, the original set of 11 confidence-building measures (CBMs) adopted in 2013 included a measure that, in part, encouraged States to hold voluntary consultations to "protect critical national and international ICT infrastructures including their integrity".[19] While adopting new CBMs in 2016, however, the OSCE focused specifically on securing CIs through a number of suggested collaborative measures. In particular, a new measure encouraged participating states, "on a voluntary basis, to encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies".

---

[18] ITU National Cybersecurity/CIIP Self-Assessment Tool (April 2009).

[19] OSCE PC.DEC/1106, ""Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies", released December 3, 2013.

19. The OSCE Decision in 2016 went to exemplify areas of collaboration as:

- "Sharing information on ICT threats;
- Exchanging best practices;
- Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;
- Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;
- Sharing national views of categories of ICT-enabled infrastructure States consider critical;
- Improving the security of national and transnational ICT-enabled critical infrastructure, including their integrity at the regional and subregional levels; and
- Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues".[20]

20. In addition, other CBMs have promulgated additional activities that could contribute to the emergence of functional CIP regimes in member states and overall cooperation in cyberspace. Thus, states were encouraged to "promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges", as well as to introduce "responsible reporting of vulnerabilities affecting the security … share[ing of] associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry". These CBMs can be seen as complementary to GGE 2015 recommendations (d),

[20] OSCE PC.DEC/1202, "Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies", released on March 10, 2016.

(g) and (j) inasmuch as they specify measures that states can adopt in pursuit of a more stable cyber environment and inter-state collaboration on securing critical infrastructures, both nationally involving relevant stakeholders, and along a critical supply-chain.

21. In the United States, the concept of "critical infrastructure" as an interconnected cyber-physical system gained prominence in the 1990s. However, it was not until the 1997 President's Commission on Critical Infrastructure Protection that this nexus, its importance for continued socio-economic prosperity and the need to mitigate CI vulnerabilities against potential cyber threats became outlined. The Commission described critical infrastructure as a complex system whose protection required joint work between governmental and private sector actors.[21] In its Executive Summary, emphasizing the criticality of the message, the Commission stated unequivocally that "infrastructure protection must be ingrained in our culture, beginning with a comprehensive program of education and awareness. This includes both infrastructure stakeholders and the general public, and must extend through all levels of education, both academic and professional".[22] On the issue of international cooperation, the Commission directly linked the success of national information assurance efforts to increased "level of international cooperation and coordination on computer intrusion matters".[23]

22. To better address these risks, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil

---

[21] *Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

[22] Ibid., page xi.

[23] Ibid., page 64.

liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework,[24] created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

23. By now, many countries in the world have adopted national cybersecurity policies and strategies, thus establishing regulatory frameworks and taking measures to improve critical infrastructure protection in line with international standards.

24. The concerns over the development of international cybersecurity norms have been shared by non-state stakeholders as well, chief among them being the corporate community. For example, Microsoft has released a number of policy whitepapers addressing both the process of norms creation, as a whole, and specific issues of concern, such as protection of critical information and national infrastructures.[25,26]

Analysis

25. The analysis of the recommendations (g) and (h) begins by clarifying their critical components, which are terms that appear to carry prescriptive or practical meaning. This enables the investigation of how these prescriptions could be translated into specific and desirable state, state agency and other relevant

[24] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014). Accessed on October 17, 2017, http://bit.ly/2jSGfcQ.

[25] Microsoft, *International Cybersecurity Norms: Reducing conflict in an Internet-dependent world* (2014) http://bit.ly/2yS65Zd.

[26] Microsoft, *Critical Infrastructure Protection: Concepts and Continuum* (2014), http://bit.ly/2yoHuul.

party behaviour, the latter including operators of critical infrastructure.[27]

Recommendation (g)

> *States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.*

Protection of critical infrastructures in a broader context of national cybersecurity

26. All experts who contributed to this analysis have agreed that recommendation (g) is important due to its preventive character. Due to the growing rates of cyber-attacks against CI worldwide and increasing reliance on ICTs, states begin to treat this recommendation as a "customary norm", i.e. its notion being already widely accepted in respective communities. Strictly speaking, it can be interpreted both as 1) calling for the establishment of national regulations for protecting various critical infrastructure sectors, such as energy, transportation, financial and others, or as 2) a recommendation to implement security measures to protect state-controlled critical infrastructures only. Taken in the spirit and context of the GGE normative rationale, the former and broader interpretation is perceived here as more accurate. However, states that opt for adopting measures in accordance with the narrower interpretation, based on their capabilities and sovereign right, would still be following the recommendation.

27. Since, in a highly-interconnected world, many critical infrastructures under public or private ownership form part of a wider information network that spans across sectors and

[27] This analysis is in part based on invaluable contributions submitted by various CIP experts specializing in physical- and cyber-security who took part in this exercise.

borders, the (in)security of one particular facility is likely to affect the state of (in)security of many others. As a sovereign international actor in cyberspace, a typical state carries the responsibility over ensuring overall security of its information systems, development of a national cybersecurity regime in partnership with CI stakeholders and communities, and collaboration with international partners on information-sharing or during crisis management. To accomplish these, and other relevant CIP tasks, the state must design and implement an effective cybersecurity governance model for CIP. Such model constructed in accordance with national strategic priorities and stakeholder interests, but also cultural and political norms, would then inform policy and regulations while ensuring rights of its citizens.

28. According to most of the expert contributors, this norm calls for the establishment of minimum levels of national ICT risk management protocols and programs to protect critical infrastructures. Based on internationally accepted best practices (e.g., NIST Cybersecurity Framework), each state is called upon to develop its own cybersecurity governance regime combined with transparent requirements for compliance and verification mechanisms to ensure adherence. Spidalieri argues that at the strategic level the focus of such a regime should be on promoting a national culture of safety, security, resilience, and stability in cyberspace.[28] Taking into consideration the existing level of threats, but also available resources and capabilities to mitigate them, the evolution of such a governance model would become more organic and linear if state authorities involve all relevant national stakeholders, including CI representatives, in this process. As cyberspace presents common threats and challenges to both government and non-government organizations, an effective private-public partnership (PPP) developed in line with national policy and institutional priorities and constraints is often seen as an effective and efficient

[28] Contribution from Francesca Spidalieri, Senior Fellow for Cyber Leadership, Pell Centre, Salve Regina University, USA.

mechanism to accomplish this task. In particular, PPP are seen as instrumental in achieving the following national objectives:

- Monitoring and identification of cyber threats, and sharing of relevant information with national and/or international partners;
- Facilitation of pooling and allocation of available expertise and resources;
- Ensuring adequate division of roles and responsibilities between government and private interests and functions; and
- Coordination of cybersecurity awareness across all segments of society, from policy makers to operators and end users, including the adoption of best practices and behaviours, which leads to the emergence of a national cybersecurity culture.

29. Predictably, the development and adoption of comprehensive national cybersecurity partnerships by individual states is an arduous process, which may lead to certain institutional and organizational variances between states, from regulatory standards to specific incident responses. At the current juncture of uneven levels of ICTs adoption, diverging priorities on state resources allocation and available human and technical capabilities, this is almost inevitable. However, this is where the international norms and bilateral or regional framework agreements promoting information sharing, transparency and cooperation measures come to the fore, providing normative expectations and strategic guidelines, respectively. Ultimately, the successful protection of national critical infrastructures would, to a significant degree, depend on harmonization of national CIP standards in line with international best practices and adoption of effective mechanisms for bilateral and regional cooperation.

30. A national approach to the adoption of "appropriate measures" to protect national CIs from cyber threats, as responsible state behavior, must begin with a shared understanding of what exactly constitutes a "critical

infrastructure"[29], with any related inter-dependencies, at a national level. It is likely that each country defines CI in direct relation to how critical a particular sector of industry, and sometimes even a particular facility, is to a country's social and economic well-being. According to Wingfield, another important step in this process is identification of the legal and political obstacles to the effective sharing of threat-based information between public and private actors in countries where such a distinction exists.[30]

31. Only after CI modalities have been analysed and designations have been developed could the discussion turn to what may constitute an "appropriate measure". In expert view, the discussion regarding appropriate measures for CIP occurs on two inter-connected levels.

32. At a tactical-technical level of CIP, the notion of "appropriate" provides a considerable degree of freedom and flexibility to national authorities in identifying and selecting protective measures. Depending on jurisdictions, these measures would be expected to meet respective threat and risk levels, available resources and capabilities, in accordance with risk management priorities set forth either by national authorities of CI Board of Directors. Since the state of perfect security is not attainable, especially given the rapid evolution of ICTs and offensive cyber capabilities, the analysis and adoption of

---

[29] According to Microsoft, critical infrastructures are: "The key systems, services, and functions (IT or physical) whose disruption, destruction, or exploitation could have a debilitating impact on public health and safety, commerce, and national security, or any combination", in *Critical Infrastructure Protection: Concepts and Continuum* (2014, page 4). available at http://bit.ly/2yoHuul. Accessed on October 18, 2017.

[30] Contribution by Thomas Wingfield, Professor of Cyber Law at the National Defence University, Washington, D.C., USA. An example of the difficulties encountered in the US by government and private stakeholders in this regard was presented by Steven R. Chabinsky, then General Counsel and CRO of CrowdStrike in his testimony to the US Congress. See testimony of Steven R. Chabinsky before the United States Senate Committee on Homeland Security and Governmental Affairs, *Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure* (March 26, 2014), at https://www.hsdl.org/?view&did=751636.

appropriate measures to protect CIs, at a single facility or sector-wide levels, constitute an integral part of the cybersecurity risk management framework development process. Johnson, argued that the main differentiating factor at a tactical level of CIP is the ever-changing threat environment to which different CIs are subjected. A standard selection of cyber risk management procedures and solutions outlined in various compliance measures, such as ISO/IEC 27001/2 suite, and managed as part of a Security Information and Event Management (SIEM) system, would be sufficient to address such threats. At the same time, he rightly points out that what may constitute an "appropriate measure" today may not be sufficient tomorrow, especially given the rapid ICT developments, transition to cloud-based infrastructures or quantum computing. In this regard, the language of the norm allows sufficient room for continued evolution of appropriate measures in both proactive and reactive stances.[31]

33. At the same time, at a higher strategic level of analysis, all contributors have agreed that the need to ensure uninterrupted functioning of inter-dependent infrastructures within and across national borders demands adoption of minimal baseline measures, as national standards. Such measures would be proscribed through regulations by relevant coordinating authorities in cooperation with industry stakeholders, and directed at protecting individual CIs while also strengthening an overall national cyber domain. Gluschke, among other experts, believes that this process must begin with the establishment of a regulatory body for ICT security and integration of cyber domain management elements into the national legislative, legal and executive branches. Apart from ensuring the necessary levels of national coordination, these steps would also promulgate a national culture for cybersecurity.[32] At this strategic level, "appropriate measures" include the

[31] Contribution by Tyson Johnson, Chief Operating Officer, Cyber New Brunswick, Canada.

[32] Contribution by Guido Gluschke, Co-Director and Senior Research Fellow, Institute for Security and Safety, Brandenburg University of Applied Sciences, Germany.

development of a National Cybersecurity Strategy, security policies and standards for CIP identifying threats, defining roles and responsibilities, information sharing protocols, minimum protective measures and other steps, including compliance mechanisms to ensure a defined (and acceptable) level of national security. This proactive approach can only be implemented if state political, regulatory and policy authorities possess the required levels of cyber knowledge and expertise to guide its development, which may not be the case in less cyber-developed nations. In such instances, cybersecurity capacity-building through education of government policy makers or engagement of a broader stakeholder base may be required, as well as reliance on international support. In some other cases, however, operators of critical infrastructures may advance the development of minimal appropriate standards and measures through a self-organized process directed through industry associations or supply chain partners. As one such example, in recent years the North American Electric Reliability Corporation (NERC) established a number of cybersecurity standards that require utilities' compliance on cybersecurity of critical infrastructures that form part of its network. On the protection of control systems, for instance, the relevant standard identifies several cyber-related vulnerabilities that exist in control systems and recommends several remedial actions (e.g., best practices).[33] While in this case NERC acted in accordance with national standards and international treaties (i.e., Canada and the United States of America), the example demonstrates that, when operators of critical infrastructures across national boundaries share a real common concern, they could impose industry-wide standards as an act of self-regulation.

34. For jurisdictions where central authorities may not be as proactive in setting minimum national standards and industries are left to develop their own in an environment of a regulatory vacuum, a real risk could emerge due to conflicting standards.

[33] NERC, CIP standards available at http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

35. In sum, the adoption of this recommendation requires national governments to consider and address the following aspects in their approaches to CIP:

- Conceptual/Strategic—understanding of the nature of cyber threats and risks to critical infrastructures in the context of global ICT development and national socio-economic priorities, and of the possible consequences of not adopting minimum security standards;
- Political—prioritization of cyber protection of CI as part of a national security agenda across the political spectrum and continuous senior political leadership attention to issues of national cyber governance and management;
- Institutional/Organizational—establishment of a national mechanism for managing cybersecurity-related activities, such as monitoring for cyber threats, sharing of relevant information and responding to incidents, in partnership with national stakeholders (PPP) and international partners;
- Capacity—fostering the development of dedicated cybersecurity expertise at all CIP levels through academic, research and other educational opportunities, exchange programs and capacity-building initiatives at national and international levels; and
- Resources—allocation of necessary resources in partnership with CI stakeholders to proactively prevent incidents and mitigate the evolving threats to CI, invest in R&D, and support the national initiatives aimed at elevating cyber preparedness and resilience.

36. Most experts agree that by advancing these combined processes, each in its own right, public and private institutions engaged in CIP would also be contributing to the emergence of a national "cybersecurity culture". This is due to the fact that, typically, the design of a sound law, policy or even operational procedure is carried out after due consideration of ethical principles, normative behaviours and inherent values such documents aim to promote among the intended audience. An

active engagement of national stakeholders across the entire private-public spectrum on CIP, and related cybersecurity matters, should therefore be aimed not only at facilitating the adoption of specific protective measures and supporting policies, but also at the cultivation of an imbedded culture of personal and communal responsibility for the cyber well-being of a society, as a whole. According to Johnson, such engagement would be better fostered through balanced messaging whereby the anxiety and concern over likely cyber incidents is countered by a positive culture of "cyber freedom" achieved by individuals deploying proactive preventive measures in self-interest, as part of an effective, national risk management framework. The empowerment of CIP constituents, from schools to senior policy officials, through effectively designed awareness campaigns might be more successful in fostering such a culture, where each plays an important support role in achieving the common success.[34]

Recommendation (h)

> *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.*

CIP across borders: sovereignty, legal frameworks and unresolved sensitivities

37. In contrast to the previously labelled "customary" norm, the adoption of recommendation (g), which at national levels is mostly seen as an undisputed requirement and necessity, the analysis of the GGE recommendation (h) produced a more complex and nuanced picture. While recognizing the spirit and relevancy of the proposed recommendation inasmuch

[34] Johnson, *op. cit*.

as it intends to enhance international cyber cooperation and stability, experts believe that, due to various legal, political and technical issues, this recommendation is more "aspirational" in nature. In other words, while the letter of recommendation (g) establishes a desirable end goal for the international community, its practical adoption is currently hindered by a plethora of unresolved issues, many of which are decidedly political in nature. Chief among these issues are the significant lack of trust and confidence between many international players as a result of border conflicts, economic competition, trans-border cybercrimes, and many other issues.

38. It must be noted, however, that experts who contributed to this analysis exhibited a considerable degree of uniformity in identifying the challenging issues and suggesting practical solutions, albeit mostly on "technical" topics. Gaps in national cybersecurity efforts imply strong risks for crucial components of the country's vital supply networks (e.g., water, electricity, telecommunications, banking) and thus social and economic stability. Furthermore, a country's weak response mechanisms to cyber threats can actually be exploited by threat actors in order to launch attacks against further countries. Given that the contributors to this commentary understand the cyber threats domain and national security imperatives pertaining to CIP, it is perhaps not surprising that the professional opinion on what "should be done" is shared across borders. With that, however, lacking awareness and leadership among senior political and legislative circles were often cited as key causes behind "action paralysis" on cyber matters in many countries due to the fact that cyber domain issues challenge the established political and managerial procedures. Such ambivalent attitudes among professionals lend a certain degree of cautious optimism with regard to the prospects of advancing this recommendation and, at the same time, also indicate that focusing on technical and pragmatic solutions, one step at a time, may prove a winning strategy in the long run.

39. The analysis of recommendation (h), therefore, would be divided into a number of sub-sections: (a) sovereignty and legality of action, (b) mechanisms of cooperation and

(c) attribution, each dealing with a critical component that underlines normative meanings and carries important practical implications.

40. Perhaps the most critical element of the norm 13 (h) is found in the second sentence, which calls States to "mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty". Undoubtedly important for its high normative value aimed at enhancing a state's own cyber capabilities and ensuring good neighbourly behaviour, the norm is based around several notions that remain problematic from legal and policy perspectives.

41. As noted by Wingfield, this GGE recommendation is the only one to explicitly mention sovereignty, one of the core principles in international law, confusion over which is a potential stumbling block in effective international cooperation.[35] While the international community has agreed that state sovereignty extends to national cyberspace, the absence of clear boundaries defining this space and the continuing practice of conducting various cyber activities below the threshold of an open conflict (e.g., espionage or counter-terrorism cyber operations) leave each state to define the application of this principle through state practice and/or treaties.[36] In this regard, activities directed against terrorist-controlled infrastructure on networks or systems located in other states, often not a party to any conflict, constitute a particularly difficult case. While these sub-threshold cyber activities should consider the sovereignty of

[35] Thomas C. Wingfield, *op. cit*.

[36] Since a full review of sovereignty is beyond the scope of this chapter, a fascinating and operationally crucial dispute within the US government casts important light on the role of sovereignty in cyberspace. For a fuller account, see Corn and Taylor, who support the notion of sovereignty as a *concept*, and the response from Schmitt and Vihul, who argue that sovereignty is a *principle*. In Corn, Gary, and Robert Taylor, *Symposium on Sovereignty, Cyberspace , and Tallinn 2.0: Sovereignty in the Age of Cyber*, American Journal of International Law, doi:10.1017/aju.2017.57, at http://bit.ly/2yv2Sxf and Michael N. Schmitt and Liis Vihul, *Respect for Sovereignty in Cyberspace* (Texas Law Review, 95: 1639, 2017), at http://bit.ly/2hMEgqk.

the states in whose territory these terrorist infrastructures reside, there is no clear answer at the moment to the key question of whether or how sovereignty proscribes such cyber activities.

42. An important nuance of this sentence is the practical interpretation of "taking into account due regard for sovereignty". Taken in the context of the entire recommendation prescribing a responsible state behaviour, this is a call on Party A (provider of assistance, at a minimum; but possibly even a conscious enabler of such malicious acts in the first place) to limit its mitigating activities within its own national borders, unless a previous bilateral assistance agreement existed with a Party B (the state affected by malicious ICT acts) allowing cross-border intrusion into the latter's cyberspace. This "outward-looking" perspective on a bilateral relationship between two sovereign actors presupposes that Party A is in full control of its own cyberspace and is thus capable, legally and technically, to mitigate malicious ICT acts emanating from its territory. In other words, in essence, recommendation (h) assumes that Party A has already adopted the prescribed measures, which a) may not always be the case due to, for example, lack of capacity, and b) opens discussion about a host of internal legal issues a country needs to consider.

43. The possible mitigation of any illegal activity inside or emanating from one's own cyberspace, apart from the obviously required intent and technical capabilities, necessitates a high degree of control over a national cyber domain and legal authority in the hands of responsible agencies. As a sovereign and internationally recognized actor responsible for national security, including in cyberspace, every sovereign state alone possesses the right to set national priorities and presumably strives to ensure that it has capabilities to enforce them. Approached from this position, the protection of national interests, with CIP ranking highly among them, is enshrined through various legal instruments and conducted under a strict rule of law—a position that extends to international cyber cooperation as well. As discussed in the previous section on recommendation (g), national cybersecurity strategies and legislations are used to assert state sovereignty over the cyber

domain by defining roles, responsibilities, priorities and taking specific actions. They are also used to outline those behaviours and activities that are deemed intolerable and illegal, like cyber-crime, child pornography or targeting of critical infrastructures, at home or abroad. Logically, it then follows that state sovereign authority can conceptually be extended onto its cyberspace, but that its full exercise becomes questionable if and when a state does not possess practical means for managing its cyber domain. These activities can be seen to include legal and regulatory provisions, but also capabilities for monitoring for threats, identifying unusual or suspicious activities (e.g., drastically increased network flooding as an indicator of a DDoS attack), conducting forensic investigations and, ultimately, punishing those who break the established laws. As another consideration, from a national security perspective, the operational management of cyberspace would be even more effective if many of these functions were to be proactive in nature, identifying and mitigating threats before real damage is incurred.[37]

44. The second part of this analysis addresses another critical component of the recommendation dealing with mechanisms of cooperation ("respond to appropriate requests for assistance/to mitigate…") which in this chapter are divided into inter-related sub-topics, information sharing and nature of responses.

45. Overall, according to Duguay, this language mirrors a number of United Nations mutual assistance treaties for law enforcement cooperation against transnational organized

[37] While beyond the scope of this chapter, it must be emphasized that the adoption of such a proactive regime must be approached carefully, with due regard to sometimes conflicting agendas between a state's desire to fulfil international obligations and maintain its national security, while ensuring the protection of citizens' rights in cyberspace.

crime,[38] corruption,[39] terrorism[40] or other commonly recognized offences.[41] As such, one could see that the GGE is following an established path to promoting international cooperation. The difference, of course, is that, while all of these activities are deemed illegal in most of the world countries, cyberspace remains a highly controversial domain with many unresolved legal and political issues. The controversial, complex and slow process of adopting an international convention on cyber-crime, known as the Budapest Convention, which was introduced in 2001, provides but one example in this regard.[42]

46. One of the challenges in both the Budapest Convention and this GGE recommendation, as they attempt to foster international cooperation on cyber issues, relates to the inherent problems associated with information sharing, both within and between countries, on cyber-related incidents. As Johnson pointedly asks, what would constitute an "appropriate request" potentially triggering an expected response?[43] In order for one state to consider providing assistance to another, the received request must be formally *legitimate*, i.e. communicated from an officially designated and authorized entity of another country using existing and trusted channels. Both states must have pre-existing and competent agencies entrusted with coordinating

---

[38] See United Nations Convention Against Transnational Organized Crime and The Protocols Thereto, (2004). Access on October 17, 2017 at http://bit.ly/1kLFaTq.

[39] See the United Nations Convention Against Corruption (2003). Accessed on October 17, 2017 at https://www.unodc.org/unodc/en/corruption/uncac.html.

[40] See the United Nations Office for Counter-Terrorism repository of international legal instruments at http://www.un.org/en/counterterrorism/legal-instruments.shtml.

[41] Contribution by Yves Duguay, President of HCiWorld and former Senior VP, Screening Operations at the Canadian Air Transport Security Authority, Canada.

[42] For an in-depth analysis, see Michael A. Vatis, *The Council of Europe Convention on Cybercrime* in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy accessible at http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf.

[43] Johnson, *op. cit.*

their respective incident management processes and bilateral agreements providing a framework for such collaboration.[44] The *content* of a request must be communicated in a language and terminology that are equally understood by both parties. While there are still many disagreements internationally on cyber issues, such as the use of cyber for military purposes, a greater consensus and common vocabulary exist among the cybersecurity community on threats, incident response, detection, recovery, and so on as it pertains to CIP. Finally, the request must also be *sufficiently detailed* with regard to the description of a crisis situation (e.g., what happened, when, how, possible damages, and actions already taken), allowing the requested party to assess the severity and develop possible responses in diplomatic and technical terms alike.

47. Evidently, the formulation of such an "appropriate request" entails the revealing of highly sensitive details regarding both the pre-attack routine operation of a critical facility, including its security measures, as well as suffered consequences. Sharing of such information, naturally, carries with it significant operational and reputational costs and necessitates the engagement of highest political, military, intelligence and technical authorities. To date, such scope of information sharing has been achieved only through bilateral or multilateral treaties aimed at the provision of mutual assistance and protection of respective infrastructures.[45] It goes without

---

[44] Operators of critical infrastructures in a similar sector across borders or internationally may develop, participate in or rely on informal information sharing networks which could be activated during crisis management. While these networks have often proven more effective during pre-incident stages on a national level, their usability for inter-state incident management is questionable. See Florian Skopik, Giuseppe Settanni, Roman Fiedler, *A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing* (Computers and Security, Vol. 60, July 2016), pages 154-176.

[45] For example, see *Agreement Between the Government of Canada and the Government of the United States of America for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security*, available at http://www.treaty-accord.gc.ca/text-texte.aspx?id=105000. Accessed on October 18, 2017.

saying that, in the current geopolitical environment, such a degree of transparency can only exist between countries that share a long and established tradition of mutual respect and cooperation. Understandably, as Wingfield points out, no written instrument will be sufficient to guarantee the assistance of a state that is the author of a malicious ICT act.[46] Here, however, international initiatives advancing confidence building measures in cyberspace, such as within OSCE and OAS, may constitute gradual processes through which making and responding to requests for assistance or mitigation would allow building confidence among states in the global cyberspace. The OSCE CBMs, for example, outline a number of voluntary measures that states could adopt proactively, such as sharing of strategies or contact information, which would provide others with indications of political intent on cyber posture, but also with information on who to contact in case of cyber emergencies.

48. Whereas the above points deal with information sharing between countries, it is important to mention that informal information sharing channels have proven themselves to be effective as catalysts for more established protocols later on. As suggested by Gluschke, increasingly in cyber incidents, information related to combating threats is not only, or even primarily, in the hands of a national government response team. In the hours and days after an incident, multiple actors—including from other countries—often contribute to identifying and then solving the issue.[47] In some instances, information sharing begins as an ad hoc collaboration, particularly during a crisis that aligns disparate sectors and even competitors toward a unified, collective response. According to the East West Institute, for example, in 2008 the Conficker Working Group came together to share information and develop a response to the Conficker worm, which had infected millions of computers around the world. Similarly, in the recent attacks against Sony Entertainment, corporate and government teams from several countries worked together to mitigate the effects of the attacks.

---

[46] Thomas C. Wingfield, *op. cit.*

[47] Guido Gluschke, *op. cit.*

Participants in these responses were willing to share information because there was a mutual benefit to be gained from the collective response, not least the trust developed between the responders, notably between government responders and private sector participants.[48]

49. With regard to the nature of responses to requests of assistance and/or mitigation during cyber incidents, a number of avenues have been proposed by contributing experts. These avenues include both technical and non-technical measures. According to Spidalieri, since ICTs and cyber issues span across all sectors and borders, states have an abundance of areas and opportunities to engage in mutual cooperation to address these issues.[49] For example, nation A could respond to nation's B request for assistance by cooperating on post-incident investigations and providing technical and financial assistance, especially if the latter lacks the domestic capacity to do so. Publicly renouncing and condemning harmful acts against critical infrastructures of a neighbouring country would also go a long way in building confidence, especially if such proclamations get supported through practical steps to assist the victim in their recovery from attacks. The provision of such assistance, however, could only occur if there is an existing mechanism for cooperation on cyber matters between states, an issue that must be approached proactively as part of national strategies for countering cyber threats.

50. If such a clear and transparent bilateral mechanism does not exist, each party would be forced or tempted to share only partial or insufficiently detailed data while expecting a full collaboration in return. This, of course, would place other parties at a disadvantage, particularly if the requested action entails the enacting of considerable measures, such as sanctions or offensive countermeasures, for example.

51. The last but not least important element in this recommendation is related to mitigating malicious ICT activity

---

[48] *Promoting International Cyber Norms: A New Advocacy Forum*, a East West Institute report, December 2015, page 13.

[49] Francesca Spidalieri, *op. cit.*

emanating from a certain territory onto another. Linked to previous discussions about sovereignty in cyberspace and the importance of bilateral cooperation agreements, the principle of limiting the misuse of ICTs within their jurisdictions that could affect the functioning of CIs in other countries, and for curbing or halting cyber-attacks against CIs originating from their own territories, is relatively well acknowledged.

52. For instance, it is assumed that states should not allow infected devices within their territory to be harnessed to conduct illegal or illicit activity against the critical infrastructure of another state. That being said, while a state may adopt this principle independently or out of regard for responsible international behaviour, the principle cannot be taken for granted, especially if the countries in question do not enjoy good relations or are not parties to a mutual cooperation agreement. When requesting from a state to mitigate suspected malicious ICT acts, the requesting party must present evidence demonstrating that such acts indeed emanate from that state's territory. In this, the recommendation touches on one of the most difficult issues in cyber domain—attribution.

53. While it is technically possible to identify sources of some cyber-attacks by IP address or "backtracing" (i.e., show that malicious DDoS traffic comes from another country), there are many other forms of malicious ICT activity that are difficult to identify or attribute unequivocally (e.g., malware), especially in cases of a state-sponsored attack using a third country as a proxy. In such instances, the affected state may have difficulties providing sufficient evidence when issuing a "request to mitigate" that would satisfy the political or public levels of "expected proof" in the country from which the attack is supposedly emanating, and would be left to rely on the goodwill of its neighbour. This, once again, reinforces the need for countries to proactively engage with other friendly states on multilateral cybersecurity cooperation agreements.

Recommendations

54. The two GGE recommendations analyzed in this chapter have the undisputed potential to enhance international cooperation on critical infrastructures protection and contribute to the emerging global cybersecurity regime. Being state-centric, the recommendations provide a general proscriptive framework for responsible state behaviour on CIP, which now needs to be operationalized by all relevant stakeholders, including corporations and international standards organizations in specific sectors, in order to sustain this international initiative.

55. Effective cyber protection of critical infrastructures, including incident response and recovery efforts, in any country depend both on the maturity of public and private sector capabilities, as well as trusted relationships to enable information-sharing and coordination between them. The concerted efforts across critical sectors and national stakeholders to identify, share and address threats emanating from ICTs and the cyber domain form part of and contribute to the continuous development of a national cyber culture, as well. Internationally, while norms can help foster trust and build confidence, they are not in themselves sufficient. Ongoing operational, functional, pragmatic cooperation and enhanced transparency around policies and response structures between states are required to ensure that norms take a permanent hold.

56. It is therefore recommended that states:

- Establish cybersecurity governance as a national priority, in particular by establishing a central coordinating body responsible for national cybersecurity governance, including on CIP matters, reporting to a key Cabinet minister, if not the PM or President themselves;
- Adopt a dedicated and comprehensive CIP framework as part of the national cybersecurity plan to outline regulatory, managerial and oversight functions for CIP, delineate clear roles and responsibilities, engage public and private stakeholders through PPP models, and take

into account all critical issues, such as information sharing and data privacy among others;

- Establish a national cyber threat centre to provide early warning for all critical sectors, complemented by emergency/incident functionalities, as well as by the capability to react appropriately and provide assistance as needed;
- Develop and use consistent language and terminology in regulations, guidance, rules and examinations to promote efficient cybersecurity planning and budget allocations (In this regard, the cybersecurity standards developed in 2014 by the United States National Institute of Standards and Technology could form the basis of this common framework);
- Establish in the national cybersecurity governance and CIP frameworks clear parameters of and inform measures and activities related to international cooperation on cybersecurity issues, including CIP;
- Develop legislation identifying illegal activities, adopt regulations and invest in technologies that can be used to stop or mitigate unlawful activities in the national cyberspace, such as malicious rerouting of Internet traffic, and make it harder for machines (within a state's sovereign networked infrastructures) to be harnessed in a botnet and used in scaled DDoS attacks against critical infrastructure;
- Introduce proactive responsibility and accountability into the marketplace through product liability that would hold manufacturers, distributors, suppliers, retailers and others who make digital products and services deployed in critical sectors (but also those available to the public) accountable for security flaws in their offerings, in particular when the security flaws are easily prevented by commonly accepted good engineering principles at that time;
- Drive innovation agendas with security, privacy, and safety requirements and standards built into their plans for new, modern national CIs;

- Require Internet Service Providers (ISPs) and the Internet Exchange (IX) community to do more to identify compromised devices, provide early warning of new infections and offer managed security services to clean up the networked infrastructures to significantly reduce, if not eliminate, the infections;
- Require ISPs and the IX community to provide authentic and authoritative routing information, by adopting secure Border Gateway Protocol routing procedures and protocols;
- Require the Internet services community (manufacturers, distributors, suppliers, retailers and others who make digital products and services) to provide authentic and authoritative naming information as part of their product interface or service. DNS trust must be established throughout the DNS hierarchy, from root servers to browsers;
- Develop and promote a national cybersecurity culture with a clear understanding that the responsibility to ensure safe and secure national cyberspace rests with every single individual and organization—public or private; and
- Launch education programs, such as security awareness training and national campaigns, motivating employees to adopt or change behaviours.

Recommendation 13 (i)

> *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.*

Caitriona Heinl

Contextualization

1. This recommendation raises three issues that are interlinked but sometimes considered separate, namely the integrity of the supply chain, the proliferation of malicious ICT tools and techniques, and the proliferation of the use of harmful hidden functions.

2. With several states having highlighted in their United Nations submissions the issue of confidence in the security of ICT products, confidence in ICT products and the integrity of the supply chain became a thread in the GGE discourse in 2009. The 2010 and 2013 reports highlight the dual-use nature of ICTs, drawing attention to their wide availability and use for either legitimate or malicious purposes. Recommendation (i) of the 2015 GGE report can be said to represent a culmination of concerns raised within the previous reports.

3. The 2010 GGE specifies that ICTs are ubiquitous and widely available, and they are neither inherently civil nor

military in nature.[1] These dual-use technologies can be used for both legitimate and malicious purposes.[2] Consequently, the purposes to which ICTs are put depend mainly on the motives of the user.[3]

4. The origin of a disruption, the identity of the perpetrator or the motivation can be difficult to ascertain.[4] Often, the perpetrators of such activities can only be inferred from the target, the effect, or other circumstantial evidence, thus enabling actors to operate with impunity.[5]

5. The 2010 GGE finds that many malicious tools and methodologies originate in the efforts of criminals and hackers, and the growing sophistication and scale of criminal activity increases the potential for harmful actions.[6] In particular, if terrorist groups acquire attack tools, they could carry out disruptive activities.[7] Proxies (such as individuals, groups or organisations like criminal organisations) can even offer an array of malicious services to State and non-State actors.[8]

6. Any ICT device can be the source or target of misuse.[9] The 2010 GGE expressed concern that the ICT supply chain could be influenced or subverted in ways that could affect the normal, secure and reliable use of ICTs.[10] Experts noted that the inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security.[11]

---

[1] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 30 July 2010 (A/65/201), page 6.
[2] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98), para. 5.
[3] A/65/201, page 6.
[4] A/65/201, page 6.
[5] A/65/201, page 6.
[6] A/65/201, para. 5-19, pages 6-7.
[7] A/68/98, para. 7.
[8] A/65/201, para. 8.
[9] A/65/201, page 6; A/68/98, para. 5.
[10] A/65/201, para. 10.
[11] A/65/201, para. 10.

7. The 2013 group re-emphasised the concern about embedding harmful hidden functions in ICTs, concluding that, as a result, ICTs "could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security".[12] These experts also recommended that States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services.[13]

8. The 2015 report further addresses the issue of hidden functions in the section of CBMs, where it encourages states to voluntarily exchange information about vulnerabilities and identified harmful hidden functions in ICT products.[14]

Background

9. As far back as the early 2000s, state submissions to the United Nations note their efforts to ensure the assessment of technical products, their security and services.[15] Overall, these submissions seem to reflect different state priorities behind supply chain security. For some States, a main concern is securing the continuity of functionality of systems and services. Others emphasise user and consumer trust in ICT products and services, while other positions include concerns about national security matters, equality, and industrial protectionism.

10. Sweden has emphasised information and network security as concerning the securing of the identities of senders and receivers, protecting information from unauthorised changes, protecting against unauthorised access to information, and

---

[12] A/68/98, para. 8.

[13] A/68/98, para. 24.

[14] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174), para. 16 (c).

[15] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 20 July 2010 (A /65/154), Qatar.

providing a reliable supply of equipment, services and information.[16]

11. Cuba has stressed that each manufacturer of informatics means must guarantee that its software or hardware does not permit hacking or generate informatics weapons capable of harming any element of information systems. Havana noted that, in general, principles and requirements such as confidentiality, integrity and availability are valid for any provision of services or manufacture of products or information and communication technologies systems. Moreover, to generate technology in a secure environment, minimum standards must be developed, including certification.[17]

12. Ukraine has noted plans for logistical and technical efforts to ensure the secure operation of all components of the country's telecommunications infrastructure.[18] The Permanent Representatives of China, the Russian Federation, Tajikstan and Uzbekistan assert in a proposed Code of conduct in 2011 that States should endeavour to ensure the supply chain security of ICT products and services, in order to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of the countries that have accepted the code of conduct, to gain independent control of ICTs or to threaten the political, economic and social security of other countries.[19]

13. A suggestion has been made by Germany to take steps to secure the trustworthiness of the supply chain for information technology.[20] Comprehensive risk management is

---

[16] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 3 July 2001 (A/56/164), Sweden.

[17] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 29 August 2002 (A/57/166/Add.1), Cuba.

[18] A /65/154, Ukraine, 20 July 2010.

[19] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikstan and Uzbekistan to the United Nations addressed to the Secretary-General, Code of conduct, pgh (d).

[20] United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international

recommended, with measures to strengthen information security on a national and global scale. Germany's 2011 Cybersecurity Strategy sets out an objective to use reliable and trustworthy information technology, and government commitments include better consumer protection by mandatory reports from software providers when they become aware of malicious codes affecting users' IT systems.[21] In addition, the speed of innovation often outpaces attempts to secure existing technologies.[22] Examples of measures to mitigate these risks include the German Federal Office for Information Security (BSI) issuance of warnings on malware and security vulnerabilities in IT products and services, its informing concerned parties (including IT vendors and general public) and provision of recommendations for countermeasures.

14. Germany has also noted that the efforts to be undertaken range from raising awareness for each single user and securing the trustworthiness of the supply chain for information technology, to responsive defences to fend off cyber attacks and an overall resilient information technology architecture.[23]

15. Belarus has raised a number of information security issues, including the potential for undeclared capabilities and vulnerabilities to appear in information security products, and a lack of capacity for detecting them in a timely fashion, which

---

security: Report of the Secretary-General", A /66/152, Germany, 14 July 2011.

[21] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 30 June 2014 (A/69/112).

[22] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 9 September 2013 (A/68/156/Add.1). *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 23 July 2012 (A/67/167), Germany.

[23] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 14 July 2011 (A/66/152), Germany.

it finds often undermines the impact of measures to protect information.[24]

16. Some States argue that ensuring full respect for the sovereign right of any State in the field of information and telecommunications includes the development, acquisition, use, import and export of, and access to, ICTs and means and related services without any restriction or discrimination. Moreover, the adoption of any measure to deny or restrict the transfer of advanced ICT know-how, technologies and means, as well as the provision of ICT services, to developing countries is argued to have possible adverse effects on their overall development.

17. By exploiting a weakness in a relatively small and weakly protected supplier, hackers can bypass even robust cybersecurity measures. The White House, assessing the cost of malicious cyber activity, observes that supply chain attack,[25] is one of three main vectors whereby hackers penetrate system defenses, accounting for over 60 percent of all adverse cyber events in 2016.[26]

18. The Global Commission on Internet Governance (GCIG) explains in a 2016 report that states and companies can implant malware or firmware during the production or installation of IT and communications systems that can then be exploited by governments or non-state actors.[27] The GCIG recommends that security cannot be treated as an afterthought and systems should be designed and deployed with security and resilience at their core, rather than trailing technological innovation.[28] Moreover, this is not an issue for governments alone. It finds

---

[24] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 11 August 2017 (A/72/315), Belarus.

[25] Defined as a firm's security flaw can put its customers, suppliers, and corporate partners at risk, page 23.

[26] https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf?lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BxuEIBmyqS92nJmFkTY95rg%3D%3D.

[27] Global Commission on Internet Governance (GCIG), "One Internet", 2016.

[28] Ibid.

that trust requires that security approaches provide assurances of resiliency against attacks (and basic privacy).[29] A proactive approach to digital security risk management is needed rather than patches after widespread implementation.[30] Colombia also specifies that governments should refrain from undermining international security standards, citing good practice within the OECD 2015 digital security risk management recommendations that are now within the country's national digital security policy.[31]

19. Similarly, an EastWest Institute (EWI) report notes the risks that can occur given the global diversity of individuals, entities, services and components and the complexity of the products and services. It finds that the deployment of cloud services, which often rely on multinational hosting and maintenance, reduces the transparency of risk.[32] Fostering and demonstrating assurance help to build and continually enhance trust among ICT buyers and suppliers.[33] Approaches to fostering assurance could include laws and regulations, contracts, independent evaluations, and transparency (although associated costs include the possible stifling of innovation).

20. As a solution, the GCIG suggests that the technical community should be encouraged to incorporate privacy- and security-enhancing solutions into all standards and protocols of the Internet.[34] Manufacturers and vendors should follow the principle of privacy and security by design and they must be prepared to accept legal liability for the quality of the technology they produce. Governments can play a role by incorporating minimum security standards in their procurement process.[35] The EWI guide finds that suppliers must secure products and services throughout their life cycle—every

---

[29] Ibid., page 53.
[30] Ibid., page 54.
[31] A/71/172, Colombia.
[32] EastWest Institute (EWI), "Purchasing Secure ICT Products and Services: A Buyers Guide", 2016, page 6.
[33] EWI, A Buyers Guide, page 16.
[34] GCIG 2016, p.15.
[35] GCIG 2016, p.15.

technology provider in the supply chain must mitigate risks along the supply chain.[36] Such efforts can include reducing the number and severity of vulnerabilities, reducing the risk of maliciously tainted code and mitigating against counterfeit components. It further recommends that ICT buyers (including governments and enterprises) and suppliers engage in a dialogue about risk management and rely on international standards to increase confidence in the results.[37]

21. It is further emphasised that many efforts are limited to managing operational risks to ICT systems and data but executives are not yet considering the impact of their purchasing decisions on the security or integrity of the technologies.[38] Many ICT buyers are not having conversations with their suppliers about how they govern and manage risk in their environments, develop technology products and services, and manage security of those over time. ICT buyers can thus enhance cybersecurity by procuring products and services that have sufficient security and integrity, as well as by factoring security into procurement decisions so that these buyers incentivise ICT suppliers to develop and provide more secure ICT.[39]

22. These decisions should be based on widely recognised international standards and best practices and they should be enforced by objective conformance regimes that are flexible and consistent with risk.[40] The EWI guide further recommends that buyers should consider collaborating with like-minded buyers to leverage their collective purchasing power and signal their collective requirements to the market. Although the guide recognises the value of international process-based standards and certifications to help assure conformance to these processes, it does not emphasise product or service certification (explaining that this may be appropriate for some technologies but can be

[36] EWI, A Buyers Guide, page 13.
[37] EastWest Institute (EWI), "Purchasing Secure ICT Products and Services: A Buyers Guide", 2016.
[38] EWI, A Buyers Guide, page 6.
[39] EWI, A Buyers Guide, page 7.
[40] EWI, A Buyers Guide, page 7.

slow and costly).[41] It finds that product certification may not sufficiently consider processes to promote version integrity and authenticity throughout the technology development and manufacturing/production life cycle and supply chain. This approach would be challenged by constantly evolving software code. It finds that one best practice gaining deeper support is the NIST Cybersecurity Framework.

23. Both the GCIG and EWI conclude that governments should not create or require third parties to build backdoors or compromise encryption standards, as this would fundamentally undermine trust.[42] Furthermore, Microsoft asserts that States should not target ICT companies to insert backdoors.[43] Otherwise this undermines the global tech industry, which is founded on trust. It explains that although the private sector invests highly in ensuring the integrity of products and services, governments can use disproportionate, large resources to exploit these products or services and to taint the broader ICT supply chain by which they are delivered.

24. Kaspersky Lab's Global Transparency Initiative highlights the need for an independent review of the company's source code, its software updates and threat detection rules, as well as the secure development life cycle processes, and software and supply chain risk mitigation strategies.

25. However, in the wake of concerns about terrorism, some governments are still calling for backdoors in hardware and software.[44] Several recent cases highlight the tension between governments and companies over access to encrypted equipment and data in cases of known terrorist activities and these examples of competing legitimate interests raise the question of how to balance the needs of law enforcement and security agencies against the need to ensure the integrity of encryption for commerce and the protection of individuals' privacy.[45]

---

[41] EWI, A Buyers Guide, page 9.
[42] GCIG 2016, page 15.
[43] Leiden consultation contribution, Microsoft, 2017.
[44] GCIG 2016, page 60.
[45] GCIG 2016, page 61.

26. Encryption is, however, viewed as the bedrock for the global digital economy. The GCIG argues that the legal default for all states should be to protect encryption and anonymity-granting technologies and any infringements on the technology should be prescribed by law and in line with the principles of necessity and proportionality.[46] It finds, however, that defining what is reasonable and practical and proportionate will not be easy. It recommends that governments should not compromise or require third parties to weaken or compromise encryption standards, for example, through hidden backdoors into the technology, as this would weaken the overall security of digital data flows and transactions.

27. The GCIG further notes that very few nations have adequate independent accountability mechanisms and judicial oversight to keep state power in check. It explains that some states and militaries are known to actively stockpile vulnerabilities, develop malware or subvert security standards, which can then be used to conduct targeted or mass surveillance.[47] Today, it is increasingly recognised by human rights experts and leading technologists that any attempt to weaken the security of the systems on which the Internet depends threatens every nation's interests.[48] The report recommends that governments should initiate efforts to develop international consensus on norms about how to deal with cases where the goal of protecting data comes into conflict with the requirements of law enforcement or security agencies to investigate terrorist activity or attacks in an emergency situation. It finds that at a minimum any solutions should be found through the multi-stakeholder process and must be subject to legal oversight, governed by principles of necessity, proportionality, and avoidance of unintended consequences.

28. The GCIG report finds that simple improvement in digital hygiene can prevent a lot of criminal behaviour, thus freeing up governmental and private resources to tackle more sophisticated

[46] GCIG 2016, page 34.
[47] GCIG 2016, page 49.
[48] GCIG 2016, page 49.

threats.[49] The report provides a number of other suggestions related to building resilience among individual and business users, including in other areas of insurance where the reliance on third party evaluators of ICT products helps to reduce systemic risk. It finds that third party evaluation processes are needed in ICT supply chains.[50]

29. A United Nations workshop report finds that strategies could focus on software or hardware design, reducing the ability of malicious actors to repurpose dual-use products for malicious purposes.

Expansion

30. Confidence-building measures (CBMs) have an important facilitating role to play also in the implementation of this norm at different levels, such as bilateral, in regional groups or other international forums. In addition to the voluntary sharing of information on vulnerabilities and identified harmful hidden functions, the 2013 GGE recommends workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from the State use of ICTs and how these incidents might develop and be managed.[51] These types of initiatives could include examining (1) how States could take reasonable steps to ensure the integrity of the supply chain to ensure end-user confidence in the security of ICT products; and (2) how to seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. Additional measures that could also strengthen supply chain security include the following: 1) sustain coordination among States to strengthen information security and share cutting-edge experiences; 2) participate in policy and regulation formulation and sharing best practices; 3) share specialised expertise and knowledge and exchanges of experts; 4) foster academic collaboration and formulate relevant programmes and

[49] GCIG 2016, page 52.
[50] GCIG 2016, page 66.
[51] A/68/98, para. 26(b).

curriculums; and 5) encourage joint research and development programmes.[52]

31. While the 2013 report explains that States should encourage and build upon progress made bilaterally and multilaterally, including in regional groups, Microsoft in its contribution emphasises that bilateral agreements, as a way forward, are not enough for a global problem. Nonetheless, States such as the Republic of Korea emphasise the importance of bilateral CBMs between major cyber powers, as well as regional measures at the ARF and OSCE.[53] Microsoft further recommends that, even where the United Nations is a core venue, alternative venues that are either new or established can supplement government negotiation—such as the London process or groups of experts could focus on how to implement norms with concrete proposals (or on how they would be enshrined in a treaty).[54]

32. As noted above, concern has recently been expressed over the potential for undeclared capabilities and vulnerabilities to appear in information security products and a lack of capacity for detecting them in a timely fashion, which often undermines the impact of measures to protect information.[55]

33. The 2013 GGE report explains the importance of capacity building to an effective cooperative global effort on security in ICTs and their use. Some States may require assistance in their efforts to, among other items, develop technical skill and appropriate legislation to fulfil their responsibilities and to bridge the divide in the security of ICTs and their

---

[52] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 9 September 2013 (A /68/156/Add.1), Oman.

[53] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 30 June 2014 (A/69/112), Republic of Korea.

[54] Leiden consultation contribution, Microsoft, 2017.

[55] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 11 August 2017 (A/72/315), Belarus.

use.[56] It recommends that States working with international organisations, including United Nations agencies and the private sector, should consider how best to provide assistance.[57] Measures to consider include: supporting bilateral, regional, multilateral and international capacity-building efforts to secure ICT use and ICT infrastructures; strengthening national legal frameworks, law enforcement capabilities and strategies; combating the use of ICTs for criminal and terrorist purposes; and assisting in the identification and dissemination of best practices.[58] The 2015 report further notes that different levels of capacity for ICT security among States can increase vulnerability in an interconnected world.[59] This group outlines that the implementation of measures (such as norm (i)) may not be immediately possible, in particular for developing countries, until they acquire adequate capacity.[60] Two countries note that there is still a need for coordinated capacity building programmes.[61]

Analysis and recommendations

34. While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society, including for supply chain security for ICT products and services.[62] State recommendations include a more consistent approach to partnering with industry to develop guidelines around conduct in cyberspace.[63] High importance is attached to involving the private sector and knowledge

[56] A/68/98, para. 30.
[57] A/68/98, para. 31.
[58] A/68/98, para. 32.
[59] A/68/98, para. 8.
[60] A/70/174, para. 14.
[61] *Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General*, 11 August 2017 (A/72/315), Singapore/United Kingdom.
[62] A/70/174, para. 31, A/68/98, para. 24.
[63] A /66/152, Australia.

institutions in this dialogue through, for instance, sharing experience and best practices.[64] Microsoft similarly finds that it is important that there be diversity of stakeholders in this process, such as industry, civil society and academia, even if the negotiation of treaties is the prerogative of government.

35. Microsoft further finds that clarity is needed around agreed-upon concepts and that many of the concepts involved in the 11 2015 GGE norms remain undefined.[65] It therefore recommends developing case studies as a means to provide practical examples of how international cybersecurity norms, such as norm (i), can be applied.[66] Singapore similarly notes, in a 2017 submission to the United Nations First Committee, the present need for well-defined norms of responsible State behaviour.[67]

36. Hill recommends that norm (i) could be implemented by agreeing to additional provisions for Article 6 of the 2012 International Telecommunications Regulations (ITRs), a treaty of the International Telecommunication Union (ITU).[68] He further recommends that, by agreeing to additional provisions for the ITRs, the Microsoft proposals for a Digital Convention and an attribution organisation could include the additional Microsoft proposals: Member States shall endeavour to refrain from inserting or requiring "backdoors" in mass-market commercial technology products; Member States shall endeavour to exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise, and not reusable; Member States shall also endeavour to also ensure that they maintain control of their weapons in a secure environment; Member States shall endeavour to agree to limit proliferation of cyber weapons; governments shall endeavour not to distribute, or permit others to distribute, cyber weapons and to use intelligence, law enforcement, and financial sanction tools against those who do; Member States shall endeavour

[64] A /66/152, The Netherlands.
[65] Leiden consultation contribution, Microsoft, 2017.
[66] Leiden consultation contribution, Microsoft, 2017.
[67] A/72/315, Singapore.
[68] Leiden consultation contribution, Richard Hill.

to facilitate the establishment of an international cyber attack attribution organisation to strengthen trust online.

37. Governments can play a further role by incorporating minimum security standards in their procurement process.[69] More consideration should be paid to the impact of purchasing decisions on the security or integrity of technologies.[70] When making purchasing decisions, government notes that, together with industry, it has been raising awareness of the threat among industry and the public so that they too demand better security in cyber products and services.[71]

38. In order not to undermine trust, governments should not create or require third parties to build backdoors or compromise encryption standards, nor should States target ICT companies to insert backdoors.[72] Instead, States should protect encryption, as well as anonymity-granting technologies, and infringements should be subject to legal oversight (adequate independent accountability mechanisms and judicial oversight to keep state power in check), governed by principles of necessity, proportionality, and avoidance of unintended consequences.

39. States should therefore continue their cooperation against criminal or terrorist use of ICTs, harmonise legal approaches, as appropriate, and strengthen practical collaboration between respective law enforcement and prosecutorial agencies. For example, General Assembly Resolution 55/63 on combating the criminal misuse of information technologies underscores the need to have modern effective national laws to adequately prosecute cybercrime and facilitate timely transnational investigative cooperation. Resolution 56/21 notes the work of international and regional organisations in combating high technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime.[73] Other countries similarly emphasise the need for effective enforcement to

---

[69] GCIG 2016, page 15.
[70] EWI, A Buyers Guide, page 6.
[71] A /68/156/Add.1, United Kingdom.
[72] Leiden consultation contribution, Microsoft, 2017.
[73] A /66/152, United States.

maintain confidence in digital society, thus encouraging more cross-border investigation with enforcement agencies and accession of other countries to the Council of Europe's Convention on Cybercrime.[74] A number of other countries, in their United Nations submissions, recommend that other states sign the Convention.

40. In addition, improving resilience with better digital hygiene can prevent much criminal activity to allow government to focus on more sophisticated threats.[75] Other ways to enhance resilience include insurance where the reliance on third party evaluators of ICT products aims to reduce systemic risk.[76]

41. While existing mechanisms have been examined and lessons may be drawn from them, experts find that there is no perfect mechanism applicable to the unique attributes of the field of cyber. Although the Wassenaar Arrangement may set a useful precedent that might, with care, be extended to cybersecurity, any extension must be mindful of the fact that there may be unintended consequences of further regulation. Alternative recommendations include legal remedies, the importance of public research conducted by organisations like the Citizen Lab, placing pressure on companies so that they become more transparent and accountable about the abuse of their products and services, and smart regulatory approaches to provide industry with guidance on what are acceptable limits in their research and development of security products. For example, one State outlines that, under an amendment to its Criminal Code on malicious software use, anyone who produces, traffics, acquires, distributes, sells or sends, or brings into or takes out of the country, malicious software or other harmful computer programmes shall be liable to a term of imprisonment and a fine.[77] Other suggestions include information sharing on malware databases, as well as government warnings on malware and security vulnerabilities in IT products and services,

[74] A /68/156/Add.1, The Netherlands.
[75] GCIG 2016, page 52.
[76] GCIG 2016, page 52.
[77] A /67/167, Colombia.

informing concerned parties (including IT vendors and general public) and delivering recommendations for countermeasures.[78]

42. Additional strategies to consider include market-based mechanisms such as bug bounty programmes, and focusing on software or hardware design.

43. Echoing the findings of the EastWest Institute report, manufacturers and vendors should follow the principle of privacy and security by design and accept legal liability for the quality of the technology they produce. Products and services should be secured by suppliers throughout their life cycle—every technology provider in the supply chain must mitigate risks along the supply chain.[79] Governments, on the other hand, should request mandatory reports from software providers when they become aware of malicious codes affecting users' IT systems.[80]

44. Microsoft suggests that other stakeholders like civil society can make progress on implementation outside government action where, for example, civil society can hold government responsible for irresponsible behaviour and industry can agree on its own set of best practices. For example, Microsoft has called for a Tech Accord that would commit the industry to, among other items, pledge not to assist any government in offensive operations, and fight the proliferation of vulnerabilities. Spain further recommends producing guides and recording good practices, in cooperation with the private sector and civil society, to support the purposes of norm (i).[81] The EWI guide is a good example of such a measure.

45. EWI finds that all stakeholders should be informed by ISOC's Collaborative Security framework. In short, laws, regulations, contracts, comprehensive risk management and international standards can enhance confidence in the trustworthiness of the supply chain.[82]

---

[78] A /67/167, Turkey.
[79] EWI, A Buyers Guide, page 13.
[80] A/69/112, Germany.
[81] A /68/156, Spain.
[82] EWI, A Buyers Guide, page 16.

Recommendation 13 (j)

> *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.*

Nicholas Tsagourias*

Contextualization

1. Due to the interconnectedness of cyberspace and the dependence of societies on ICT, vulnerabilities can jeopardise international peace, security, stability and prosperity and undermine the values that underpin cyberspace. More specifically, vulnerabilities can be exploited to attack or undermine states and their people and thus threaten international peace, security and stability. The exploitation of vulnerabilities for malicious or hostile purposes can also impose significant economic, social, political, and legal costs on individuals, societies, industry, corporations, and states. The GGE has concluded that, if unaddressed, vulnerabilities undermine trust and confidence in cyberspace, which are necessary commodities to maintain its values of openness, interoperability and

* Professor Nicholas Tsagourias, University of Sheffield (Nicholas.Tsagourias@sheffield.ac.uk). The Lead Editor wishes to thank Louis Léonet for his invaluable assistance with the preparation of the commentary.

vigorousness, and to realise its full potential.[1] Vulnerabilities also undermine trust and confidence in the ability or willingness of governments and private or public sector organisations to secure cyberspace. For these reasons, detecting, reporting and remediating vulnerabilities is critical in order to maintain a secure, open, interoperable, vigorous and reliable cyberspace, but also in order to foster and maintain trust and confidence in this medium and in its stakeholders.

2. The 2010 GGE Report did not address this issue directly. The Report stated that vulnerable technologies and harmful hidden functions in ICT affect secure and reliable ICT use, trust and security. It also opined that such vulnerabilities can be amplified due to disparities in national law, regulations and practices related to the use of ICTs.[2] The 2013 GGE Report did not mention responsible reporting as an activity that can mitigate such threats and risks. The promulgation of more detailed "norms, rules and principles for the responsible behaviour of states" in the 2015 GGE Report builds on the 2010 GGE Report. The aim of these norms, rules and principles is to address and neutralise risks to international peace, security and stability. Recommendation (j) thus belongs to a "family of activities" to prevent, mitigate or neutralise existing and emerging threats, risks and vulnerabilities and to promote an open, secure, stable, accessible and peaceful ICT environment.[3] More specifically, it is part and parcel of a group of recommendations, namely (c), (h), (i) and (k), which demonstrate that securing cyberspace is a shared responsibility.

---

[1] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174), para. 2; Final Report of the Global Commission on the Internet: One internet (2016) https://www.cigionline.org/initiatives/global-commission-internet-governance.

[2] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 30 July 2010 (A/65/201), para. 5-10.

[3] A/70/174, para. 13.

Background

3. Vulnerabilities are almost everywhere in cyberspace. According to Symantec, 76% of scanned websites in 2016 contained vulnerabilities, with 9% being critical vulnerabilities.[4] According to ENISA, over 1,900 high-severity vulnerabilities and around 5,356 medium-severity vulnerabilities were reported in 2014, which represented almost 92% of all reported vulnerabilities in 2014.[5] Their exploitation can cause serious cybersecurity incidents. As a matter of fact, there is an ever growing vulnerabilities market for legitimate or nefarious purposes.[6] In what follows, I will present a number of well-publicized incidents of vulnerabilities exploitation to illustrate the point that exploitable vulnerabilities pose a serious threat to cybersecurity.

4. A case in point is the WannaCry ransomware attack in 2017, which affected thousands of computers in many countries, including Spain's Telefonica and the United Kingdom National Health Service. The WannaCry attack exploited a vulnerability found in Windows' Server Message Block (SMB) protocol to create encrypted data and demand a ransom in order to decrypt them. The infection vector was released by the hacker group Shadow Brokers, stolen from the Equation Group, which is broadly believed to be tied to the United States National Security Agency (NSA). When Microsoft discovered the vulnerability,

---

[4] Symantec, *Internet Security Threat Report* (No. 22, April 2017) page 33. Available from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf; see also the Council of Foreign Relations' Cyber Operations Tracker https://www.cfr.org/interactive/cyber-operations.

[5] European Union Agency for Network and Information Security (ENISA), *Good Practice Guide on Vulnerability Disclosure: From challenges to recommendations* (January 2016), p.17. Available from https://www.enisa.europa.eu/publications/vulnerability-disclosure.

[6] Bruce Schneier, *The Vulnerabilities Market and the Future of Security* (Forbes 30 May 2012); Lillian Ablon, Martin C. Libicki, Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Research Report, RR-610-JNI, Santa Monica, CA., RAND Corporation, 2014), page ix (e.g.). Available from https://www.rand.org/pubs/research_reports/RR610.html.

it released patches for its Windows operating systems.[7] It is widely believed that the NSA was aware of the vulnerability but did not disclose it to Microsoft in order to exploit it for its own purposes.[8] It was claimed that the WannaCry attack was linked to the Democratic People's Republic of Korea.[9]

5. In 2014, the existence of the *Heartbleed* bug was disclosed. The bug exploited vulnerabilities in the OpenSSL cryptography library that allowed attackers to read confidentially encrypted data and to take the encryption keys used to secure the data.[10] It was claimed that, although the NSA was aware of the vulnerability, it failed to disclose it,[11] an allegation denied by the NSA.[12]

6. In 2012, the *Shamoon* virus exploited the Windows NT kernel to attack Saudi Arabia's Aramco systems in an

---

[7] Microsoft Security Bulletin MS17-010—Critical (10 November 2017): https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

[8] Victoria Woollaston, *WannaCry ransomware: what is it and how to protect yourself* (Wired, 22 May 2017). Available from http://www.wired.co.uk/article/wannacry-ransomware-virus-patch.

[9] Ellen Nakashima, *The NSA has linked the WannaCry computer worm to North Korea* (Washington Post, 14 June 2017). Available from https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.09d739e3c1a2.

[10] Alex Hern, *Heartbleed: Hundreds of thousands of servers at risk from catastrophic bug* (The Guardian, 9 April 2009). Available from https://www.theguardian.com/technology/2014/apr/08/heartbleed-bug-puts-encryption-at-risk-for-hundreds-of-thousands-of-servers; Jane Wakefield, *Heartbleed bug: What you need to kno*w (BBC, 10 April 2014). Available from: http://www.bbc.co.uk/news/technology-26969629; Jeff Sass, "The Role of Static Analysis in Heartbleed" White Paper, (SANS Institute, 2015), esp. sect. 1.3. Available from http://www.sans.org/reading-room/whitepapers/threats/role-static-analysis-heartbleed-35752.

[11] Michael Riley, *NSA Said to Have Used Heartbleed Bug, Exposing Consumers* (Bloomberg, 12 April 2014). Available from https://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.

[12] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities* (White House Blog, 28 April 2014).

unprecedented attack erasing data in two thirds of Aramco's PCs.[13] The attack caused severe disruption to the business operation of the company but it did not affect the oil production and did not cause any physical damage.[14]

7. The *Stuxnet* attack in 2010 was another incident where a worm exploited the Microsoft Windows Shortcut "LNK/PIF" vulnerability to infect Siemens programmable logic control software used to operate the Iranian nuclear reactors and give different instructions.[15] This led to approximately 984 machines taken out of service.[16]

Expansion

8. There are a number of policy documents that deal with the issue of responsible reporting and of sharing information about remedies. Most private organisations have policies on responsible reporting that can be found on their websites.[17] The International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) have also published guidelines and standards on vulnerabilities disclosure

---

[13] Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back* (New York Times, 23 October 2012). Available from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[14] Christopher Bronk & Eneken Tikk-Ringas, *Hack or Attack? Shamoon and the Evolution of Cyber Conflict* (Working Paper, James A. Baker III Institute for Public Policy, Rice University, 1 February 2013), p. 3. Available from https://www.bakerinstitute.org/media/files/Research/dd3345ce/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf.

[15] Chloe Albanesius & Larry Seltzer, *Report: Stuxnet Worm Attacks Iran, Who is Behind It?* (PCMag.com, 27 September 2010). Available from https://www.pcmag.com/article2/0,2817,2369745,00.asp.

[16] John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield* (J. Marshall J. Computer & Info. L., N°29 (1) (2011)), page 11. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888.

[17] For Microsoft, see: https://technet.microsoft.com/en-us/security/dn467923.aspx; for IBM see: https://www.ibm.com/security/secure-engineering/report.html.

and handling.[18] They include guidelines on mechanisms for submitting reports, the information that should be included in the reports, the contact information, including secure means of contact, the processes for verifying and analysing the reports, and the processes for handling and resolving vulnerabilities. They also refer to policies on disclosing vulnerabilities and on deploying remediation, policies on communication with other stakeholders, and on follow-up processes.

9. It is difficult to verify the extent to which states have developed specific policies on responsible reporting and exchange of information on remedies. The reason is that such policies, if they exist, are often kept secret. However, demands for transparent policies on responsible disclosure already exist. The Netherlands has published a *Policy for Arriving at a Practice for Responsible Disclosure*.[19] The aim of the policy is "to bring together disclosers with knowledge of vulnerabilities and the desire to remedy them, and the organisations affected by them and that are dependent on these vulnerable systems".[20] The policy defines responsible disclosure as revealing ICT vulnerabilities in joint consultation between discloser and organisation based on a responsible disclosure policy set by the organisation.[21] It includes a chapter on the responsibilities of the parties and another chapter on the building blocks for responsible disclosure.

---

[18] International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) "Information technology—Security Techniques - Vulnerability disclosure", document ISO/IEC 29147:2014(E). Available fromhttp://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip.
ISO/IEC, «Information technology—Security techniques—Vulnerability handling processes», document ISO/IEC 30111:2013. Available from https://www.iso.org/standard/53231.html.

[19] The Netherlands, Ministry of Security and Justice, National Cyber Security Centre, *Policy for Arriving at a Practice for Responsible Disclosure* (The Hague, 2013), page 3. Available from: https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

[20] Ibid.

[21] Ibid., page 5.

10. The Austrian Cyber Security Strategy (2013)[22] provides that a comprehensive report analysing the need to establish an additional legal basis, regulatory measures and voluntary self-commitment (Code of Conduct) for guaranteeing cybersecurity in Austria will be prepared and submitted to the federal government, which would also cover the issue of information exchange between authorities and private persons, and their reporting duties. It goes on to say that:

> The responsibility of using digital technology in a prudent way rests with each individual organisational unit. But it is only broad cooperation between all sectors and a permanent mutual exchange of information that will make the use of ICT transparent and safe. It is therefore important to strengthen existing capacities and processes in the administration and economy as well as among citizens through cooperation and to create new opportunities.[23]

11. In France, Article 47 of the Law for a digital Republic, Chapter I of Title II of Book III of Part Two of the Defense Code, is supplemented by Article L. 2321-4 as follows:

> Art. L. 2321-4. For the purposes of the security of information systems, the obligation laid down in Article 40 of the Code of Criminal Procedure is not applicable in respect of a person of good faith who transmits to the national authority only security of information systems information about the existence of a security vulnerability of an automated data processing system.
>
> The authority shall preserve the confidentiality of the identity of the person who originated the transmission and the conditions under which it was carried out.
>
> The authority may carry out the technical operations strictly necessary for the characterization of the risk or threat mentioned in the first paragraph of this article to

[22] Austria, Federal Ministry of the Interior, *Austrian Cyber Security Strategy* (Vienna, 2013), sect. 5.2. pages 12-13. Available from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf.

[23] Ibid.

warn the host, the operator or the person in charge of the information system.[24]

12. In Germany, the Federal Office for Information Security (BSI) published recommendations for software vendors concerning vulnerability handling.[25] It puts emphasis on the "principle of 'coordinated disclosure' (also referred to as 'responsible disclosure') when publishing information on vulnerabilities" and continues by saying that "'coordinated' means that a vulnerability is reported confidentially. The researcher who discovered it cooperates with the vendor to develop a proper update and information on the vulnerability is disseminated after remediation of the threat."[26] It includes recommendations on internal preparation, setting up communication channels, the actual incident handling and the post-processing phase.

13. In the United Kingdom, vulnerabilities were handled via GovCert and CERT-UK but in order to improve the vulnerability disclosure process, the National Cyber Security Centre (NCSC), which is part of Government Communications Headquarters (GCHQ), launched the *Vulnerability Co-ordination Pilot* with the participation of an invited group of United Kingdom–based security practitioners to learn lessons as to how vulnerabilities across three publicly facing systems used in United Kingdom Public Sector can be identified and resolved.[27]

---

[24] Translated from: France, Law n° 2016-1321 of 7 October 2016 pour une République numérique, Art. 47, Title II, Chap. 1, sect. 1. Available from https://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo/article_47; see also Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)'s vulnerability disclosure portal : https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/.

[25] Germany, Federal Office for Information Security (BSI), *Vulnerability Handling: Recommendations for Software Vendors* (2012). Available from https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_019E.pdf;jsessionid=FC8CAE514926104E2E40B5CBDA55C91C.2_cid341?__blob=publicationFile&v=2.

[26] Ibid., page 1.

[27] United Kingdom, GCHQ, National Cyber Security Centre, *Vulnerability Co-ordination Pilot,* Blog post (13 March 2017). Available from https://www.ncsc.gov.uk/blog-post/vulnerability-co-ordination-pilot.

14. ENISA published a *Good Practice Guide on Vulnerability Disclosure* for EU member states.[28] The document identifies a number of challenges regarding vulnerability disclosure, which include legal challenges; lack of vendor "maturity"; lack of researcher "maturity"; incoming vulnerability reports not always being taken into consideration by the vendors; vulnerability acquisition for national intelligence purposes; users not implementing patches (in a timely manner); and varying discoverer motivation. It then identifies a number of good practices concerning communication, information dissemination, timelines, flexibility in reporting and disclosing and finally makes recommendations. The core recommendations are: the community must facilitate the improvement of vendor maturity; internationalisation through policy learning; introduction of a neutral third party or enhancement of existing coordination centres; European policy makers and Member States should improve the legal landscape; vendors should facilitate trust building, transparency and openness; and finally, ENISA should facilitate and advise to improve the vulnerability disclosure landscape.

15. The *CERT Guide to Coordinated Vulnerability Disclosure*, compiled by Carnegie Mellon University, provides a comprehensive and detailed description and analysis of the processes. It does not represent the official United States Governmental position but it is a "summary of what we know about a complex social process that surrounds humans trying to make the software and systems they use more secure. It's about what to do (and what not to) when you find a vulnerability, or when you find out about a vulnerability".[29] It contains chapters on the principles of coordinated vulnerabilities disclosure (CVD), roles in CVD, Phases of CVD, and Process Variation.

---

[28] ENISA, *Good Practice Guide* (2016).

[29] Allen D. Householder, Garret Wassermann, Art Manion & Chris King, *The CERT® Guide to Coordinated Vulnerability Disclosure*, Special Report, CMU/SEI-2017-SR-022 (Software Engineering Institute, Carnegie Mellon University, August 2017), p. ix. Available from https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

16. The Vulnerabilities Equities Policy and Process for the United States Government (VEP) declassified in November 15, 2017 deals with the issue of determinations about disclosure or retention of new vulnerabilities discovered by the United States Government. The Policy is biased toward disclosure unless there is "demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes."[30] The Policy also makes it clear that the process is not binary but includes other options such as disseminating mitigation information to certain entities without disclosing the particular vulnerability, limiting the use of the vulnerability by the United States Government in some way, informing United States and allied government entities of the vulnerability at a classified level, and using indirect means to inform the vendor of the vulnerability. The VEP review is an inter-agency process coordinated by the NSA. It includes an Equities Review Board, an Executive Secretariat and a VEP Director at the NSA.[31] The Policy applies to all United States Government components and personnel (i.e., civilian, military, and contractors) and includes Government off-the-shelf (GOTS), Commercial off-the-shelf (COTS), or other commercial information systems (to include open-source software), Industrial Control Systems (ICS) or products, and associated systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).[32] Only "newly discovered and not publicly known vulnerabilities" fall within the VEP.[33] Decisions are made by consensus or, if such consensus is not achieved, by voting on a preliminary determination that can however be challenged.[34] The policy also lays down a number of considerations taken into

[30] United States, *Vulnerabilities Equities Policy and Process for the United States Government* (VEP), unclassified (White House, 15 November 2017),sect. 1. Available from https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[31] Ibid., sects. 4.1 - 4.2.

[32] Ibid., sect. 3.

[33] Ibid., sect. 5.1 and annex A.

[34] Ibid., sect. 2.4, 2.6

account when making determinations. They include "Defensive Equity Considerations"; "Intelligence, Law Enforcement, and Operational Equity Considerations"; "Commercial Equity Considerations"; and "International Partnership Equity Considerations".[35] A limited category of vulnerabilities are excluded from VEP review, but which categories these are remains classified.[36]

17. There has been some commentary on the VEP. Ari Schwartz and Rob Knake, former members of the National Security Council (NSC), make a number of recommendations to ensure oversight, transparency and accountability.[37] According to their recommendations, the VEP should be adopted by the President by means of an executive order in order to formalize it and thus ensure government-wide compliance; the high-level criteria that will be used to determine whether to disclose or retain a zero day vulnerability should be made public; the process to be followed in making a disclosure decision should be clearly defined; periodic reviews of retained zero day vulnerabilities should be introduced; agencies should be prohibited from entering into non-disclosure agreements with vulnerability researchers and resellers; the Executive Secretary function should be transfered from NSA to the Department of Homeland Security; the Executive Secretary should be directed to issue a public report on an annual basis on the status of the program; Congressional oversight of the government's use of vulnerabilities should be expanded; oversight by independent bodies within the Executive Branch should be mandated; and funding for both offensive and defensive vulnerability discovery and research should be expanded.[38]

---

[35] Ibid., annex B.

[36] Ibid., sect. 5.4.

[37] Ari Schwartz and Rob Knake, *Government's Role in Vulnerability Disclosure* (Discussion Paper, The Cyber Security Project, Belfer Center for Science and International Affairs, June 2016), sect. 2. Available from https://www.venable.com/files/Publication/a609d60e-ffcf-4ec4-8bca-e5b7160a1cc3/Presentation/PublicationAttachment/0729f804-8242-4a77-a50a-e82b9f32f27f/Governments-Role-in-Vulnerability-Disclosure.pdf.

[38] Ibid., pp. 13-17.

18. Based on research conducted by a team of researchers, Jason Healey discusses the United States VEP and makes certain estimates as to the zero-day vulnerabilities retained by the United States. As he states "our best estimate, with moderate confidence, is that prior to the 2014 'reinvigorated' policy the U.S. government retained dozens of vulnerabilities per year" but "we estimate with high confidence that in the period from 2014 to today, the U.S. government retains single-digit numbers of vulnerabilities per year." Moreover, "we estimate with moderate confidence that the current U.S. arsenal of zero-day vulnerabilities is probably in the dozens." He recommends that VEP should include a presidential mandate that agencies may not use discovered vulnerabilities until it has been approved for retention by the ERB; an active industry perspective in VEP should be included; quarterly and yearly statistics should be made public to improve transparency; the risk mitigation plan when a vulnerability is retained should be released. [39]

19. The *Protecting our Ability To Counter Hacking (PATCH) Act*[40] was introduced to the Senate in May 2017 to formalise the VEP into law. The PATCH Act designates the Department of Homeland Security instead of the NSA as the chair of the interagency review board. The role of the Board is to decide whether, when, and how a non-public vulnerability can be disclosed. The Bill lays down several criteria to inform such decisions but they are not categorised on the basis of importance. The Bill establishes oversight mechanisms and improved transparency and accountability mechanisms including annual reports to the Senate. The Bill requires periodic review of all non-public vulnerabilities and not only of the newly discovered ones. However, in its decision whether to disclose, it also takes

---

[39] Jason Healey, *The U.S. Government and Zero-Day Vulnerabilities: From pre-Heartbleed to Shadow Brokers* (Columbia Journal of International Affairs, SIPA, November 2016), pages 15-17. Available from https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process

[40] United States of America, Senate, *A Bill To establish the Vulnerability Equities Review Board, and for other purposes,* a.k.a. PATCH Act, BAG17434 (115th Congress, May 2017). Available from https://www.schatz.senate.gov/imo/media/doc/BAG17434_FINAL%20PATCH.pdf.

into account whether the private company has a disclosure policy.[41]

Analysis

20. Recommendation (j) twines together two more specific modalities that are separate but also related. The first is responsible reporting of vulnerabilities and the second is exchange of information about remedies. The first describes an internal process whereby a state encourages ICT stakeholders to responsibly report vulnerabilities whereas the second describes an external process where states exchange information on remedies.

21. Academic commentary on recommendation (j) is rather meagre but, according to one commentator, this recommendation requires states to report vulnerabilities to other states and to exchange information about remedies with other states.[42] According to said commentator, the recommendation regulates interstate relations. In the opinion of the Lead Editor, such an interpretation stretches the content of the recommendation as far as its reporting prong is concerned and is not supported by the text of the recommendation. The position of the Lead Editor based on a textual analysis is that recommendation (j) requires states to encourage responsible reporting by third parties within their jurisdiction and these third parties are all relevant ICT stakeholders within the state's jurisdiction. This interpretation is also in line with the scope of the recommendations preceding or following recommendation (j), which mention actions that a state should take within its own jurisdiction.[43] Furthermore, the summary provided at the beginning of the 2015 GGE Report states that "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

[41] Mailyn Fidler and Trey Herr, *PATCH: Debating Codification of the VEP* (Lawfare, 17 May 2017). Available from https://www.lawfareblog.com/patch-debating-codification-vep.

[42] Contribution by Anatoly A. Streltsov.

[43] Recommendations (h), (i) and (k).

of malicious ICT tools, techniques or harmful hidden functions",[44] which definitely confines the implementation of this recommendation within the state's jurisdiction. Finally, the interpretation put forward by the Lead Editor also finds support in the Dutch policy on responsible reporting, according to which it is only organisations that should engage in responsible disclosure and not states. It is also supported by the states' cybersecurity policies mentioned above. To this it should be added that, as will be explained subsequently, it is the vendor who is often a private company that receives reports on vulnerabilities and should disclose such vulnerabilities to stakeholders and provide remedies.

22. A critical question is whether governmental agencies should report to vendors the vulnerabilities they may discover. The dilemma facing them is obvious because not reporting them may facilitate the government's law enforcement or national security tasks but, at the same time, it may undermine the security of its cyber infrastructure and of its users. The requirement to report vulnerabilities is general and applies to governmental agencies as well. As was also seen above, certain states have set out relevant processes concerning reporting of vulnerabilities by governmental agencies.

23. The GGE Report does not provide a definition of vulnerabilities, allowing technical definitions found in other documents to be used here. A vulnerability has been defined as "a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy".[45] The NIST defines vulnerability as "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat *source*."[46] Microsoft defines

---

[44] A/70/174, para. 2.

[45] R. Shirey, *Internet Security Glossary*, Internet Engineering Task Force (IETF) (2000), page 189. Available from http://www.rfc-base.org/txt/rfc-2828.txt.

[46] Richard Kissel (Editor), United States of America, Department of Commerce, National Institute of Standards and Technology (NIST), *Glossary of Key Information Security Terms,* NISTIR 7298 (Revision

a security vulnerability as "a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product."[47] A vulnerability is in other words a property that affects the resilience of a system and, more specifically, its availability, integrity and confidentiality.[48] It should be further noted that vulnerabilities refer to product (software or hardware) weaknesses and not to an instance where a product is vulnerable.[49]

24. It should be further noted that the aforementioned definitions of vulnerabilities are not legal or binding. Individual organisations may adopt their own definitions of vulnerabilities.[50] It thus becomes apparent that the absence of common definitions and understandings can affect the scope of recommendation (j). It also transpires from the above that, although specifically enumerating vulnerabilities is a rather futile exercise, holding a database of vulnerabilities assists in their management.[51]

25. Recommendation (j) employs the term "responsible reporting of vulnerabilities" but often the terms vulnerabilities disclosure, responsible disclosure of vulnerabilities or coordinated vulnerabilities disclosure are used interchangeably. These terms describe a more inclusive process beyond the act of reporting and, in the view of the Lead Editor, the term "responsible reporting" employed in recommendation (j) is synonymous with disclosure of vulnerabilities. If responsible reporting is confined to the act of reporting, the aims behind the recommendation will not be served. The view that responsible

---

2, May 2013), page 212. Available from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

47 Microsoft Developer Network (MSDN), Definition of a Vulnerability. Available from https://msdn.microsoft.com/en-us/library/cc751383.aspx.

48 The Netherlands, NCSC, Policy for *Arriving at a Practice for Responsible Disclosure*, page 4.

49 CERT Guide to Coordinated Vulnerability Disclosure, sect. 1.2.7.

50 For a review of definitions, see ENISA, Good Practice Guide (2016), sect. 2.2.

51 See e.g.: NIST's National Vulnerability Database. Available from https://www.nist.gov/programs-projects/national-vulnerability-database-nvd.

reporting implies something broader is supported by the second leg of recommendation (j), which requires states to exchange information about remedies. It is the public disclosure of vulnerabilities and of their remediation after they have been reported that would allow states to share information about remedies with other states, as will be explained later.

26. Responsible reporting is a process that encompasses several phases: discovering vulnerabilities, reporting vulnerabilities to relevant stakeholders, remediation, disclosing the existence of vulnerabilities and their resolution to consumers and the general public, and the deployment of remediation.[52]

27. It also transpires from the above that responsible reporting is an iterative process. It involves many stakeholders performing different roles and tasks but who may also have competing interests. These include finders (reporters/disclosers); organisations (developers/vendors/users); and government.[53] A finder is the person who discovers a vulnerability, whereas the discloser/reporter is the one who reports it, although they may be the same person. A finder (discloser/reporter) can be a researcher, vendor, user, or third parties such as individuals or cybersecurity companies. The recipient of the report is usually the vendor, that is, the organisation that created the programme where the vulnerability was found, but can also be an agency created to coordinate the process within a sector or a national agency such as CERTs. The vendor or relevant other organisations are tasked with finding a remedy and with deploying the remediation. The finder, vendor or coordinating agency can disclose the vulnerability and any remedies.

28. Disclosure of vulnerabilities and sharing information with users or the wider public about remedies can take the form of an advisory report or bulletin that contains information about

---

[52] CERT Guide to Coordinated Vulnerability Disclosure, p. xiii & sect. 4.

[53] Ibid., sect. 3 & 6; United States of America, Department of Commerce, National Telecommunications and Information Administration (NTIA), *Multistakeholder Process: Cybersecurity Vulnerabilities* (15 December 2016). Available from: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

the vulnerability, the affected products, the impact of the vulnerability, and its remediation. The timing of such disclosure is important and depends on whether the vulnerability is exploited or not, whether remediation is available, and whether other stakeholders are involved.[54] Different organisations have different time-frames.

29. Defining what constitutes responsible reporting is central to implementing recommendation (j). In the first place it should be noted that the qualification "responsible" does not allude to moral responsibility but to judiciousness or reasonableness of the decision by taking into consideration all the equities. In this sense, it is not a purely subjective judgement but is relatively objectified on the basis of certain tests. As was also noted above, the term coordinated disclosure of vulnerabilities or disclosure of vulnerabilities is used to avoid any suspicion of subjectivity.[55]

30. Responsible reporting is not an absolute value but is intended to strike the right balance between security and insecurity—the security it provides through knowledge of vulnerabilities and their neutralisation or mitigation, and the insecurity caused by their exploitation or potential for exploitation.

31. Responsible reporting is reporting that satisfies certain qualitative criteria and thresholds. First, the information provided should be technically accurate, sufficiently detailed, and reasonably complete in order to facilitate effective action. Second, responsible reporting does not require immediate reporting but can justify a time-lapse between the discovery of the vulnerability and its reporting in order to assess the security risk posed and determine whether remedies can be applied. It is advisable that disclosure and resolution should coincide in time and that a deadline exists, after which disclosure takes place. Third, the type of disclosure may be qualified or be full, including exploits or Proof of Concept script.

---

[54] BSI, *Vulnerability Handling: Recommendations for Software Vendors*, page 4.

[55] ENISA, Good Practice Guide (2016), sect. 2.5.

32. Responsible reporting by governments may take into account additional factors such as: the immediacy of the risk of exploitation; whether the vulnerability can affect networks supporting national critical infrastructure; whether the anticipated harm from the exploitation of the vulnerability by other states or malicious actors will be significant; whether the vulnerability is known to adversaries or malicious actors; whether it is possible to know whether others know of the existence of the vulnerability or whether they can discover it; how important the exploitation of the vulnerability by the state that discovered it is; and what the purposes for exploiting the vulnerability are.[56]

33. These factors do not necessary make decisions easier in the absence of concrete knowledge and information and in the absence of some type of hierarchy between the factors.[57] Instead several questions can be asked; for example, how can harm or the different types of harm inflicted on different stakeholders be assessed and measured? Is harm on critical infrastructure more important compared to harm on individuals? How close or remote should such harm be and how can future harm be foreseen? Furthermore, what capabilities are needed to determine whether others can discover the vulnerability and to what extent such judgment is affected by the ever-developing

---

[56] Michael Daniel, op. cit.; Trey Herr, Bruce Schneier, *Rediscovering Vulnerabilities* (Lawfare, 21 July 2017). Available from https://lawfareblog.com/rediscovering-vulnerabilities; Mailyn Fidler, *The Vulnerability Equities Process Should Consider More than Intelligence Community Needs* (Just Security, 2 September 2016). Available from https://www.justsecurity.org/32697/vulnerability-equities-process-intelligence-community/; Lillian Ablon & Timothy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (Santa Monica, CA., Rand Corporation, 2017). Available from https://www.rand.org/pubs/research_reports/RR1751.html.

[57] Tristan Caulfileld, Christos Ioannidis and David Pym, *The U.S. Vulnerabilities Equities Process: An Economic Perspective*, in: *Decision and Game Theory for Security,* S. Rass , B. An, C. Kiekintveld, F. Fang, S. Schauer, eds. 8th International Conference *GameSec 2017* (Vienna, Austria, October 23-25), Proceedings (Springer, Cham). Available from http://www0.cs.ucl.ac.uk/staff/D.Pym/VEP.pdf (alternative: https://link.springer.com/chapter/10.1007/978-3-319-68711-7_8).

technology, and who are these "others" who may discover the vulnerability? Are they adversary states or malicious actors and which actors? Does the possibility of using the vulnerability against adversaries weigh more than disclosing it? An important issue is also the level of confidence a government should have in its assessment: what level of knowledge should a government possess regarding the life cycle of a vulnerability? Finally, to what extent is the decision to disclose or retain vulnerabilities affected by a state's investment in exploitation technologies, and what knowledge should exist about the availability and speed with which patches can be applied?

34. In sum, in order for responsible reporting to achieve its purpose, its aims and underlying principles need to be clearly defined;[58] it needs to be iterative, involving relevant stakeholders and also needs to be properly managed with participants, roles, decision-making chains and mechanisms being clearly identified and regulated. It also needs to be timely, transparent, and accountable.

35. An issue that can affect the process of responsible reporting is the demand for legal non-disclosure agreements. Although different organisations may have different non-disclosure policies, it should be stressed that such agreements may discourage the discovery and reporting of vulnerabilities and thus affect the effectiveness of this recommendation. It should be recalled in this regard that national policies or recommendations often take a negative view towards the need for such agreements.[59] Another important issue is the legal liability of finders such as researchers.[60] To the extent that finders act within the law and adhere to relevant procedures,

---

[58] CERT Guide to Coordinated Vulnerability Disclosure para./sect. 2 identifies the following coordinated vulnerability disclosure principles: Reduce Harm, Presume Benevolence, Avoid Surprise, Incentivize Desired Behavior, Ethical Considerations, Process Improvement.

[59] BSI, *Vulnerability Handling: Recommendations for Software Vendors*, p. 2.

[60] Katie Moussouris,*Vulnerability Disclosure Deja Vu: Prosecute Crime Not Research* (Dark Reading, 12 May 2015). Available from http://www.darkreading.com/vulnerabilities---threats/vulnerability-disclosure-deja-vu-prosecute-crime-not-research/a/d-id/1320384.

no liability should be incurred. Prior authorisation will remove any criminal or civil responsibility, provided of course that all activities follow legal or other rules. The French criminal law mentioned above is a good example of facilitating discovery and reporting of vulnerabilities or the taking into account in any process of the ethical dimension of hacking.[61]

36. Although, as was said, recommendation (j) does not require states to report vulnerabilities to other states, a requirement to disclose vulnerabilities to other states can be inferred from recommendation (c) on due diligence. The duty of due diligence encompasses a duty to inform or warn other states of potential or impeding harms, as the International Court of Justice held in the *Corfu Channel* case.[62] Such a duty of informing has been specifically recognised in certain areas of international law such as in environmental law.[63] It can thus be contended that, to the extent that a general duty to inform, notify or warn exists in international law, it translates into a duty to inform other states of vulnerabilities that may cause damage to their infrastructure. The contours of such a duty in cyberspace need to be further clarified; for example, does such a duty arise only if the prospective damage is serious? A requirement to notify can also be inferred from recommendations (d) on notification and (h) on assistance. That having been said, the view that this recommendation requires states to exchange information with

---

[61] France, Art. 47 of Law n° 2016-1321. See also ANSSI's vulnerability disclosure portal.

[62] *Corfu Channel Case (United Kingdom v. Albania), Judgment, I.C.J. Reports 1949*, pp. 4, 22.

[63] *Trail Smelter Case, (United States of America v. Canada), Arbitration Award of 11 March 1941, RIAA III,* para. 1965; Principle 21 of the *Report of the United Nations Conference on the Human Environment,* Stockholm, Sweden, 5-16 June 1972 (United Nations publication, Sales No. E.73.II.A.14 and corrigendum) ; Principle 2 of the Report of the United Nations Conference on Environment and Development, Rio de Janeiro, 3-14 June 1992, vol. I, Resolutions Adopted by the Conference (United Nations publication, Sales No. E.93.I.8 and corrigendum) *Legality of the Threat or Use of Nuclear Weapons*, *Advisory Opinion*, *I.C.J. Reports 1996*, p. 22, para. 29; *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay),Judgment*, *I.C.J. Reports 2010*, p.14, para. 101, 193.

each other about remediation is correct, in view also of the technological inequalities between states.

37. Regarding the second prong of recommendation (j), namely, the sharing of information about remedies, this is an interstate obligation and, in the opinion of the Lead Editor, it particularises the content of other recommendations contained in the 2015 GGE Report. More specifically, it particularises recommendation (a) according to which states should 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; recommendation (c) on due diligence; and recommendation (d) according to which 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. All these recommendations seek to ensure peace, security and stability in cyberspace. The role of the second prong of recommendation (j) in this respect becomes evident in view of the differences in technological development and capacity between states.

38. In order for the sharing of information on remedies to be effective, points of contact need to be established between states with national CERTs playing such role. International cooperation through international organisations such as the United Nations or the ITU or specifically established agencies within these organisations can streamline the exchange of information about remedies.

39. However, there are certain issues that affect the content and scope of this particular aspect of recommendation (j). First, remedies are disclosed and deployed by vendors, which are usually private organisations. They are disclosed to all their consumers/users or to the public in general, regardless of nationality or territory. In this respect, the role of the state in exchanging information about remedies becomes redundant unless the second prong of recommendation (j) refers to disclosure by governments. Secondly, if states should exchange

information about remedies, the immediate question is whether technologically advanced states should transfer knowledge and technological know-how to technologically less advanced states and what assistance they should provide in order to deploy remedies. In the view of the Lead Editor, these are issues falling within the scope of recommendations (a), (c) and (d). Third, questions may be asked as to the scope of such exchange in light of differences in legislation and in practices concerning ICT security. States may be reticent to share all information about remedies or to provide assistance for national security reasons, but receiving states may also be reticent to accept such assistance for national security reasons.

40. The commentary will conclude by looking into the subjects of recommendation (j) as well as its status.

41. The subjects of recommendation (j) are states due to the fact that the 2015 GGE was mandated to promote common understandings of responsible behaviour by states. In an environment such as cyberspace, where non-state actors are not only visible but perhaps even more powerful than states, the GGE's approach may be criticised as being under-inclusive. However, it should be recalled that only states are members of the United Nations and only states have the power to legislate; consequently, only states can implement this recommendation at the international or domestic level.

42. Although the legal status of the recommendations contained in the 2015 GGE Report has been discussed in the Introduction, it is important to comment on the nature of any obligation[64] recommendation (j) may impose on states. If it were to impose obligations, these will include an obligation of conduct and an obligation of result. The phrase "states should encourage responsible reporting" implies an obligation of conduct in that the implementation of this aspect of recommendation (j) requires positive intervention by the state to encourage responsible reporting by individuals or private

[64] The word 'obligation' is used here in a quite broad sense to describe 'should' as well as 'ought'. The legal status of the 2015 GGE recommendations has been examined in the introduction.

or public organisations and agencies within its jurisdiction. The state is not obligated to achieve a result (responsible reporting) but it will fail in its obligation if it remains idle. The second part of the recommendation, namely that states should share associated information on available remedies to such vulnerabilities, imposes an obligation of result in that states should share such information and would fail in their duty if they fail to share information on remedies.

Recommendations

43. Encouraging responsible reporting and exchanging information about remedies involves various actions by states, such as:

- States should encourage software companies to introduce responsible reporting policies, including remediation and deployment policies. Responsible reporting should cover the life cycle of a product, including its development cycle.
- States should publish and disseminate standards and best practices for responsible reporting and invite ICT stakeholders to voluntarily abide by them.
- States should facilitate the creation of platforms where policies, guidelines or standards concerning the process of discovery, reporting, and disclosure are discussed and endorsed by key stakeholders. These policies should also cover the handling of private data, cooperation between internal and external agencies, communication with third parties, anonymity, whistleblowing, rewards, and prosecution.
- States should adopt national policies on responsible reporting based on generally agreed standards and good practices. States should gradually build them into law and establish oversight, accountability and enforcement mechanisms.

- States should put in place an institutional framework to coordinate and streamline responsible reporting. States should establish a focal point to receive and assess reports and decide on further action. States should also establish troubleshooting processes.
- States should introduce an enabling legal framework to facilitate responsible reporting by balancing society's need for cybersecurity with the rule of law. Because of the interconnected nature of cyberspace, states should engage in dialogue with other states within international fora to establish common legal frameworks for responsible reporting.
- States should promote international collaboration to devise and inculcate best practices or rules and regulations on responsible reporting and sharing of information.
- States should develop policies regarding responsible reporting by governments and establish oversight and accountability mechanisms. They should enter into dialogue and share information on their policies with other states.
- States should promulgate laws or reinforce existing laws with regard to disclosure, retention or use of vulnerabilities.
- States should establish focal points to receive information about remedies.

Recommendation 13 (k)

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Eneken Tikk

Contextualization

1. Recommendation (k) in the 2015 GGE report builds on the United States' input.[1] It addresses the independence of national computer security incident response teams[2] that, in the United States' view, is essential to national and/or economic security concern of all states as it should prevent malicious cyber activity.[3]

2. Recommendation (k) opens a new theme in the United Nations GGE. Although several risk areas are pointed out in

---

[1] See Brian Egan, *Remarks on International Law and Stability in Cyberspace* (2016), page 8. Available https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf.

[2] OAS defines CSIRT as a team or an entity within an agency that provides services and support to a particular group 1 (target community) in order to prevent, manage and respond to information security incidents. See Organization of American States, Best Practices for Establishing a National CSIRT (2016), available at https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf.

[3] Brian Egan, op. cit., page 8.

the 2010 and 2013 reports, there is no specific mentioning of the independence of CSIRTs or concerns about the inviolability of their information systems. The 2013 Group only notes that exchanges of information and communication between national Computer Emergency Response Teams (CERTs), within CERT communities, and in other forums are essential to support dialogue at political and policy levels.[4]

3. The 2015 report, however, pays extended attention to the topic of first responders. The Group calls for the establishment of national computer emergency response teams, cybersecurity incident response teams or other officially designated organizations to fulfill this role.[5] It further recommends expanding and supporting practices in computer emergency response team and cybersecurity incident response team cooperation.[6]

4. Further in line with recommendation (k), the 2015 report suggests that considering first response and incident mitigation capacity within national definition of critical infrastructure would strengthen cooperation on a bilateral, sub-regional, regional and multilateral basis.[7] The Group recommends that States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies.[8]

5. Recommendation (k), generally building on the widely and repeatedly expressed need to upgrade national incident prevention and response capabilities, differs from all other recommendations due to its relatively strong direction, narrow

---

[4] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 24 June 2013 (A/68/98), para. 26 (d).

[5] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by Secretary-General, 22 July 2015 (A/70/174), para. 17 (c).

[6] A/70/174, para. 17 (d).

[7] A/70/174, para. 17 (c).

[8] A/70/174, para. 17 (c).

focus and somewhat opaque background considerations. In addition to suggesting that there is an acute concern about the inviolability of the first response capability and pointing to (potential) inappropriate uses of CERTs/CSIRTs, it also makes a recommendation to include this capability among critical national resources. It is precisely this focus that the following commentary will address.

Background

6. There is little explanatory material available about the immediate considerations behind emphasis on the inviolability of incident response capability. Of course, with various cyber incidents being a concern, CSIRTs' systems are potential targets just like their constituencies'.[9] However, as network and data security is CSIRTs' core competence, recommendation (k) hardly serves as a mere reminder. In this context, further considerations are essential.

7. The United States International Strategy for Cyberspace discusses the first response capability in the context of *dissuasion*. Here, incident response acquires a cross-border defence dimension, whereby the ability to recognize and respond to incidents is seen as a crucial step in denying would-be attackers the ability to do lasting damage to [United States] national and international networks. Concluding that a globally distributed network requires globally distributed early warning capabilities, the United States commits to producing new computer security incident response capabilities globally, and to facilitate their interconnection.[10]

8. According to Professor Streltsov, authorized CERTs are an important element in the formation of the *system of international*

[9] This is underscored, for instance, in ENISA's report on *Strategies for Incident Response and Cyber Crisis Cooperation* (2016), page 4.

[10] White House International Strategy for Cyberspace (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, page 13.

information security.[11] He notes that the main objective of the "Center for Computer Emergency Response" is to reduce the level of information security threats for users of the Russian segment of the Internet (hereinafter referred as the Center).[12] In this context, President Putin recently addressed the need to implement an effective capability to detect, prevent and mitigate computer-based attacks against Russian information resources in the context of Russian critical information infrastructure protection.[13]

9. Normally, CERT cooperation is a routine technical matter, to the point where no special international arrangement has been necessary to establish links and communication between dozens of national counterparts.[14] Between the United States and Russia, however, the theme of CERT cooperation has been elevated to the highest strategic attention. In June 2013, the Russian and the United States presidents agreed three bilateral CBMs, one of which addressed links between their Computer Emergency Response Teams:

> To facilitate the regular exchange of practical technical information on cybersecurity risks to critical systems, we are arranging for the sharing of threat indicators between the U.S. Computer Emergency Readiness Team (US-CERT), located in the Department of Homeland Security, and its counterpart in Russia. On a continuing basis, these two authorities will exchange technical information about malware or other malicious indicators, appearing to

---

[11] According to *Basic Principles for State Policy of the Russian Federation in the field of International Information Security to 2020* (2013): para. 7 International information security system is defined as a set of national and international institutions, which should regulate activities of different actors of the global information space. International information security system should counter threats to strategic stability and facilitate equitable strategic partnership in the global information space.

[12] Ibid.

[13] http://pravo.gov.ru/laws/acts/101/545048.html and http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.787596436144353#0.

[14] See FIRST (www.first.org).

originate from each other's territory, to aid in proactive mitigation of threats. This kind of exchange helps expand the volume of technical cybersecurity information available to our countries, improving our ability to protect our critical networks.

10. Without strategic context, this measure could be read as trivial and insignificant. However, the steps taken by Obama and Putin were "designed to increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship".[15] In other words, any bilateral arrangements between these strategic contestants are surgical fixes to mutually acknowledged and prioritized issues.

11. There is also very little evidence of actual incidents against first responders. As one of the contributors to this commentary notes, any possible state activities against CERTs and CSIRTs would rarely become public.[16] However, as the same commentator emphasizes, intelligence agencies can be assumed to monitor adversaries' CSIRTs. The 2014/2015 Group may have concluded that incident response capability's nexus with defence and intelligence interests is likely to make them subject to other states' interest and, to draw attention to the issue, offered recommendation (k) as a precautionary measure.

12. Further to defence and intelligence interests vested in first responders, CERTs and CSIRTs have also faced accusations for cooperation with law enforcement agencies. Bradshaw observes CSIRTs are increasingly becoming enmeshed in the emergence of a broader cyber regime complex. Teams no longer form a single regime of actors operating in an environment characterized by shared norms, beliefs and procedures. Instead, they must operate in a high-stakes environment shared with other institutions and organizations that have their own distinct

---

[15] The White House, *FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security* (17 June 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

[16] Contribution by Robert Morgus.

and sometimes divergent laws, interests and cultural contexts.[17] The problem is deepened where CERTs and CSIRTs are expected or required to fill the functions of law enforcement or intelligence agencies, or will be perceived as acting in such a capacity.[18]

13. In 2015, Carnegie Mellon University (CMU), host of the Computer Emergency Response Team Coordination Center (CERT/CC), one of the world's most important hubs for coordinating information about various cybersecurity vulnerabilities and attacks, was reported helping FBI to crack Tor, the secure browsing application used by privacy-conscious Internet users for both legal and illegal activities.[19] Although not directed at another government, this incident stresses the need to draw a clear line between CERTs/CSIRTs and national law enforcement authorities.

14. The CERT/CSIRT community, traditionally established on trust and mutual consideration, has been put under elevated scrutiny and pressure due to the politicization and securitization of cyber issues in the past decade. Accordingly, it is essential to de-conflict between their core functions and their possible utility as power instrument.

Expansion

15. The United States original framing of recommendation (k) emphasizes the need not to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents and avoid using CSIRTs to enable online activity

---

[17] Samantha Bradshaw, Global Commission on Internet Governance, *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity* (Paper Series 23, December 2015), available at https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf.

[18] Ibid.

[19] Robert Morgus, *The FBI Should Stop Undermining Norms Before They Take Root*, Just Security Blog, 15 December 2015, available at https://www.justsecurity.org/28343/fbi-stop-undermining-norms-root/.

that is intended to do harm.[20] Morgus regards the definition of "harm" one of the key elements of the recommendation. A thorough elaboration of "harm" remains beyond the scope of this commentary. Suffice to say that, when implementing recommendation (k), cyber attacks directed at first responders' networks are the minimum interpretation, whereby a maximum agenda would include maintaining the trust, integrity and independence of their own national CERTs and CSIRTs, and those of others.

16. Streltsov notes that the lack of coordinated universal international procedural norms regulating investigation of security breaches against information systems of CERTs will create difficulties in discussing results of the analysis with other states as well as non-party states to engaged regional security systems.[21] In this comment, the Russian concern for the need of adaptation of international law reappears, testifying to their unease with situations that do not fall under the existing rules letter by letter. In this context, it is essential to consider whether the prohibition in recommendation (k) can be fully implemented on the basis of existing international law and state practice.

17. The CERT/CSIRT community has been established on trust and mutual consideration. The trends of politicizing and securitizing cyber issues in the past decade has put the incident response community under elevated scrutiny and pressure. In the light of the increasing volume and sophistication of cyber incidents, there is a strong push for creating not only incident management, but also response and cybersecurity operations capacity across the world. This requires guidance, coaching and capacity building from the already established teams. At the same time, the ever-increasing risks and vulnerabilities of the interconnected system and the way of modern, smart life require constant upgrade and sustainment of operational capabilities. The community of first response often becomes the

[20] A State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents. A State also should not use CSIRTs to enable online activity that is intended to do harm.

[21] Contribution by Anatoly A. Streltsov.

community of all coordination in case of a major cyber incident. In developing their capabilities, especially towards anticipatory and predictive functions of preventing cyber incidents, CERTs often constitute considerable ears, eyes and hands when it comes to new attack trends, capabilities and motivation. OAS observes that teams that arose primarily to respond to incidents have evolved and are now frequently oriented to a comprehensive model of information security management.[22]

18. Bradshaw summarizes the challenges for international cyber incident response cooperation. First, she observes the commercialization of cybersecurity and the commodification of vulnerabilities such as zero-days that have contributed to a competitive, rather than collaborative, approach to cybersecurity.[23] This goes against the considerate and trusted spirit in which first responders have historically operated. Second, states are increasingly recognizing the Internet as a new domain in which to exert control. Rather than cooperating with each other and with other actors in the emerging cyber regime complex to strengthen the security of the network, state actors are increasingly hoarding their knowledge of vulnerabilities and other threat-related information that could help CSIRTs prevent and respond to incidents.[24] The emphasis here is on the potential of alienating CSIRTs from their respective governments and blindsiding the community because of competing political interests. Third, CSIRTs are increasingly becoming enmeshed in the emergence of a broader cyber regime complex. Teams no longer form a single regime of actors operating in an environment characterized by shared norms, beliefs and procedures. Instead, they must operate in a high-stakes environment shared with other institutions and organizations that have their own distinct and sometimes divergent laws, interests and cultural contexts.[25] The problem is deepened where CERTs and CSIRTs are expected or required to fill the functions of law enforcement or intelligence agencies, or will be perceived

[22] Organization of American States, op. cit.
[23] Samantha Bradshaw, op. cit.
[24] Ibid.
[25] Ibid.

as acting in such a capacity. Finally, Bradshaw observes, the CSIRT community itself is growing. The importance of the Internet and our dependency on it have increased not only the stakes but also the number of players with interests in protecting and securing the network. Thus, not only are new CSIRTs being socialized into the CSIRT community, where they must coordinate with one another, but the CSIRT community is also being socialized into the broader cyber regime complex, where they must cooperate with a broad range of actors who hold diverging interests.[26] Elevated political pressure and increasing workload further pushes a more bureaucratic and politicized approach to CERT functions and operations.

19. Uninterrupted and trusted capacity of incident prevention and handling is crucial to preventing and mitigating all aspects of cyber threat. Their capacity and tradecraft make the first response community a valuable point of coordination and exchange for both their own government's law enforcement and intelligence agencies, and those of foreign governments. However, blurred lines between the incident response, law enforcement and intelligence functions may easily jeopardize the relative success that the CERT/CSIRT community has achieved in international cooperation on prevention and mitigation of malicious and hostile activities online. Whenever a cyber threat materializes in their jurisdiction, CERT and CSIRTs work to minimize its effects on the population, corporate and government affairs. They may also be requested to assist other governments or non-government entities in preventing a likely or imminent incident.

20. To understand and implement this GGE recommendation, Morgus, Skierka, Hohmann and Maurer raise a number of considerations. They conclude that effectively implementing the GGE's recommendation in question requires a better understanding of the CSIRT landscape.[27] However, Morgus et al

---

[26] Ibid.

[27] Robert Morgus et al., National CSIRTs and Their Role in Computer Security Incident Response, (2015), available at http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__

also note that effecting the norm raises a number of questions. The first set of their issues pertains to the term "authorized". What does "authorized emergency response teams" mean? Can any CSIRT, or only national CSIRTs, be authorized by a state and thereby be included under the protective umbrella of this norm? Can a state simply authorize a CSIRT and then communicate that authorization? Or does the authorization process include some sort of peer review or recognition?[28] Morgus et al problematize the types of activities condemned in the recommendation. What constitutes "harm," as used in the report? Does unauthorized access to an information system constitute harm? Similarly, what constitutes "malicious international activity"?[29] Finally, they recommend exploring more closely the idea that a state should not prevent a CSIRT from providing assistance.

Analysis

21. As a country may have more than one CSIRT, it becomes essential to consider whether all of them fall within the area of application of recommendation (k). On the one hand, the norm seeks fundamental and comprehensive protections to the incident prevention and handling capability. In this reading, the proper and unhindered functioning of all CERTs and CSIRTs can be presumed to be in national interest.

22. OAS summarizes eight main ordering functions of CSIRTs: academic, commercial, governmental, critical infrastructure,

---

November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf. On this, see also See also, Isabel Skierka et al, CSIRT Basics for Policy-Makers: The History, Types and Culture of Computer Security Incident Response Teams (2015), available at http://www.gppi.net/fileadmin/user_upload/media/pub/2015/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf. See further, Henk Bronk et al, A step-by-step approach on how to setup a CSIRT (2006), available at https://www.enisa.europa.eu/publications/csirt-setting-up-guide, and Klimburg and Zylberberg, Cyber Security Capacity Building: Developing Access (2015), available at https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf.

[28] Morgus et al, op. cit., pages 6-7.

[29] Ibid.

national, military, provider-specific and SME.[30] ENISA defines Computer Security Incident Response Team (CSIRT) as an organization that receives reports of security breaches, conducts analyses of the reports and responds to the senders. It observes that a CSIRT may be an established group or an *ad hoc* group of experts. However, ENISA notes that other widely accepted terms exist for CSIRTs, such as CERT (Computer Emergency Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team) or SERT (Security Emergency Response Team).

23. The core task of incident response and management is the protection of an organisation's information by developing and implementing an incident response process (e.g., plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and then effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems.[31] Generally, the main role of the national or governmental CSIRT should be supporting the management of security incidents for systems and networks within its state's borders.[32]

24. ENISA notes that the roles and responsibilities of the CSIRT, its relationships with other national public and private stakeholders in the national cybersecurity landscape and Incident Response (IR) practice should be defined, ideally in a national cybersecurity strategy.[33] National legislation, however, allows even fuller clarity of the mandate, resources as well as status of the national CSIRT. In this author's view, legal authorization should be preferred so as to allow for maximum legitimacy and transparency of the act of authorization. OSCE, in the context of international cybersecurity, encourages States to have in place modern and effective national legislation to

[30] Organization of American States, op. cit., page 15.
[31] ENISA, op. cit., page 7.
[32] Ibid., page 10.
[33] Ibid., page 10.

facilitate co-operation and effective, time-sensitive information exchange between competent authorities.[34]

25. Further to national authorization, external communication of such authorization needs to be considered. Here, related recommendation of OSCE provides additional guidance:

> Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily 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. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.[35]

Fifty-seven states, by this recommendation, have emphasized that authorization, both internal and external, can be expected 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.

26. Formalizing the capability of CSIRTs will provide the element of "authorization" in recommendation (k). Further building on ENISA's note that a CSIRT may be an ad hoc expert group, it is also essential to appropriately mandate and authorize any teams that are managing an ongoing incident. In this context, it is essential to note that often, in case of an ongoing incident, assistance is lent by CSIRTs and individual experts of third countries or international organizations. Therefore, clearly formulating the routine functions and setup of

---

[34] OSCE PC.DEC/1202, "Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information And Communications Technologies", released on March 10, 2016, para. 6.

[35] Ibid., page 1.

CSIRTs, as well as their expansion or setup under out-of-routine circumstances, is key to defining the area of protection when seeking to implement recommendation (k). This commentary to recommendation (k) regards national and governmental CSIRTs as the primary object of the proposed protections. It excludes sectorial and thematic (including military/defence), as well as privately operated, entities from the discussion.

27. Clear authorization is also paramount to establish the independence of CSIRTs. As discussed above, the nexus of incident response capability with national defence authorities raises the question of the independence of first responders. OAS refers to a military CSIRT as one that provides services to the military institutions of a country. Their activities are usually limited to the defense, or offensive cyber capabilities, of a nation. In addition to standard incident response technologies, they often have specific ICT knowledge for military use including, for example, weapons and radar systems.[36] In this context, the call for abstaining from harming the functioning of such capability, and the recommendation to categorize CSIRTs as national critical objects, can be read as inviting a special status to CSIRTs under international law.

28. There are other functions of CSIRTs that would require additional legal clarification. For instance, in the European Union, where IP addresses are, under certain conditions, regarded as personal data, CSIRT activities that go beyond general technical monitoring and situational awareness analysis might result in personal data protection claims.[37]

29. Concluding on the account of authorization, a definitive authorization of the object (the appropriate entity, community or other setup) and the subject (its tasks and functions) needs to be established at national level and communicated to other states.

---

[36] OAS summarizes eight main ordering functions of CSIRTs: academic, commercial, governmental, critical infrastructure, national, military, provider-specific and SME (see Organization pf American States, op. cit., page 15).

[37] See Andrew Cormack, Incident Response and Data Protection (2011), available at https://www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf.

30. The second part of this analysis elaborates on the scope of protections ordered by recommendation (k). In this context, it is essential to note the two-way expectation expressed by the Experts. According to the second sentence of recommendation (k), a state should not use authorized emergency response teams to engage in *malicious international activity*. The first sentence of the recommendation calls states to not conduct or knowingly support activity to *harm* the information systems of the authorized emergency response teams.

31. Although the recommendation itself does not clarify the relationship of these two terms and requirements, there seems to exist one. The recommendation can be read as extending authorized CSIRTs certain privileges and immunities. In this reading, authorization alone cannot be the sole basis of granting them. Accordingly, the question of inviolability of CSIRTs becomes one of reciprocity and conditions.

32. In this context, the second part of the recommendation sets an additional qualifying requirement to the protections sought after. It would be hard to conceive how CSIRTs that engage in malicious international activity could be immunized from other governments' reactions or counteractions. While this author does not suggest that the two conditions—a CSIRT engaging in internationally malicious activity and harm to its information systems—should co-occur for the recommendation to be implemented, she offers a reading whereby affording any protections to CSIRTs should occur under the presumption that they do not, on their part, engage in harmful activities.

33. Morgus et al underscore the essence of explaining the concepts of "harm" and "malicious international activities" as used in recommendation (k). As the GGE has not defined these terms, this commentary relies on their general meaning.[38] Curiously, the terms appear largely synonymous in common language. According to Merriam-Webster, malicious as an adjective refers to "having or showing a desire to cause harm

[38] Adamson, in her commentary to recommendation (c), offers a discussion of 'harm' in the context of the norm of due diligence.

to someone". Harm, according to the same source, refers to physical or mental damage. The term *international* could be understood, for the purposes of the recommendation, as cross-border, especially absent globally accepted criteria of malicious activities in the context of both state and non-state uses of ICTs.

34. Accordingly, recommendation (k) invites a two-way restraint: on the one hand, CSIRTs should abstain from activities that damage interests of other states. On the other hand, states should abstain from intentions and practice to damage the functioning of CSIRTs. The defining criterion in recommendation (k) vis-a vis both harm and damage is that they are attributable to a state. In case of a non-state actor, intruding into or otherwise targeting CSIRT systems would be regarded as a matter of criminal law. As crime remains outside of the mandate of the GGE, it can be concluded that recommendation (k) concentrates on the harm and malicious activities where a state actor is involved (a) by incentivizing or requesting CSIRT to engage in activities that are likely to be regarded as malicious by other states or the international community or (b) by taking action against another country's CSIRT.

35. One can approach the concept of damages and harm from the legal perspective. Adamson discusses the concept of harm in international law in the context of due diligence. However, the standards of harm that are outlined in international law and legal practice are all inconclusive when it comes to cyber activities. There is not enough settlement to know for sure whether something would be accepted as harmful or damaging in a particular jurisdiction or by international community.

36. As to the final point Morgus et al raise, that a state should not prevent a CSIRT from providing assistance, this seems to fall well within the spirit of recommendations (a) and (d) on cooperation and assistance.[39]

[39] Morgus et. al., op. cit.

Recommendations

37. To implement recommendation (k), it is useful to recall the recommendations of Morgus and Maurer:

- To protect trust in these teams is not place them under the control of law enforcement and intelligence agencies;
- Clarify their mandates and missions;
- Express their mandates, missions, contacts to relevant international communities.

ISBN 978-92-1-142326-6

17-22949