CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Confidence Building Measures for Cyberspace – Legal Implications

Dr Katharina Ziolkowski

Tallinn 2013

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre) and it represents the views and interpretations of the Centre. This publication does not represent the opinions or policies of NATO and is designed to provide an independent position.

Third-party sources are quoted as appropriate and the Centre is not responsible for the content of the external sources referenced in this publication. The Centre assumes no responsibility for any loss or harm arising from the use of information contained in this publication. Copies of this publication may be distributed for non-profit and non-commercial purpose only.

Contact

NATO Cooperative Cyber Defence Centre of Excellence

Filtri tee 12, Tallinn 10132, Estonia

publications@ccdcoe.org

www.ccdcoe.org

Contents

1. Introduction

The present paper[*] describes the nature of confidence building measures (CBMs) and illustrates the current developments within the international community which aim to elaborate such measures for cyberspace. Based on the political discourse of States, as reflected by the sets of adopted, recommended or currently drafted CBMs, this study interprets international law as it applies to cyberspace in the realm of international peace and security, and offers an insight into legal implications for CBMs. For the purposes of the present analysis, cyberspace is understood as a global, non-physical, conceptual space, which includes physical and technical components, i.e., the internet, the 'global public memory' contained on publicly accessible websites, as well as all entities and individuals connected to the internet. Cyberspace has political, economic, social and cultural aspects going far beyond the notion of a pure means of information transfer.

CBMs are a verified instrument of international politics, which aims to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis situation. CBMs achieve this by establishing practical measures and processes for (preventive) crisis management between States. Due to the specific features of the internet, the development of CBMs for cyberspace proves to be difficult. As indicated by current discussions, CBMs for cyberspace will display the nature of political commitments. Political declarations of States are a powerful tool of international relations. Importantly, they are significant for the progressive development of international law, especially within the realm of 'general principles of international law', which establish (in an abstract and general manner) several obligations of States, which are partly addressed by the existing sets of (draft) CBMs for cyberspace. A political commitment to CBMs for cyberspace concluded at a regional, or broader, international level, will support the concretisation of the respective general principles of international law, and thus establish their obligatory nature in terms of applicable 'hard law'. Additionally, the present paper elaborates the significance of CBMs for cyberspace for the North Atlantic Treaty Organization (NATO) and proposes a (secondary) role for the organisation with regard to their development.

However, before presenting the above-mentioned aspects in more detail, it is of the utmost importance to acknowledge the politico-historic context of CBMs for cyberspace. It not only mirrors the dynamics within the international community with regard to international peace and security in the cyber realm, but also influences the current CBMs negotiations.

[*] The present paper contains information on the development of confidence building measures for cyberspace as of 1 September 2013. Due to limited research resources, the assessment of secondary legal sources is primarily based on scholarly writings available online. The author is deeply indebted to the NATO ACT – SEE Legal Office for providing access to various online databases.

2. Politico-Historic Context

The end of the Cold War coincided with several strategic decisions of the United States (US) government, and with technical developments, which laid the foundations for the transformation of the academic research networks, which were mainly geographically based in the US, into the internet as it is known today.[1] Two decades later, the internet is deemed a truly global network, indispensable to political, economic, social and cultural life in post-industrial States. At the same time, a revival of Cold War metaphors in the context of cyberspace is perceivable in the media and in political and legal science.[2] Indeed, the perception of cyber security, formerly viewed as an exclusively technical and organisational challenge, has undergone a strategic shift. Cyber security has become an inherent part of national security, as evident by the multitude of national cyber security strategies issued[3] since 2008, and thus also a matter of international peace and security.

Some States emphasise the potentially deadly characteristics of cyber tools and the risk of cyberspace transforming into a new global battlefield.[4] Indeed, the armed forces of several States tend to consider cyberspace the fifth domain of warfare (beside land, sea, air and

[1] The US decommissioned the Advanced Research Projects Agency Network (ARPANET), initially developed by the US Department of Defence for collaboration in the context of scientific defence research projects (28 February 1990), and disconnected the US Computer Science Network (CSNET) (October 1991). The US agency National Science Foundation (NSF) opened the succeeding main network (NSFNET), which subsequently built the backbone of the internet, for other than academic or educational purposes (March 1991). The introduction of the first World Wide Web service of hyperlinked documents, i.e., websites, by a CERN scientist shaped the current feature of the net (6 August 1991). See Johann-Christoph Woltag, 'Internet' in Rüdiger Wolfrum (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press 2008, online edition [www.mpepil.com]) [in following MPEPIL] MN 2; National Science Foundation, 'A Brief History of NSF and the Internet' (Factsheet, 13 August 2003) <http://www.nsf.gov/news/news_summ.jsp?cntn_id=103050>; Vincent Cerf, 'How the Internet Came to Be' (1993) <http://www.virtualschool.edu/mon/Internet/CerfHowInternetCame2B.html>; CERN, 'The birth of the web' <http://home.web.cern.ch/about/birth-web>.

[2] eg Noah Schachtman and Peter W. Singer, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive' (Brookings Institution Paper, 15 August 2011) <http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx>; David Singer, 'In cyberspace, New Cold War' *The New York Times* (24 February 2013) <http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?pagewanted=all>; Yasmin Tadjdeh, 'U.S. Engaged in "Cyber Cold War" with China, Iran' *National Defence Magazine* (7 March 2013) <http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1075>. For scientific contributions see eg Matthew Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale Journal of International Law 425-426; Brandon Valeriano, 'Mind the Gap? Deterrence in Cyberspace' *New Atlanticist* (11 July 2012) <http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace>.

[3] See selection of publicly available strategic cyber security documents at NATO CCD COE, National Strategies & Policies website <http://ccdcoe.org/328.html>.

[4] eg the Chinese statement at the United Nations General Assembly, noting that the 'international community […] must work to prevent the information space from becoming a 'new battlefield'', UN Doc A/DIS/3467 (1 November 2012); Sergey Fedosov, 'Statement by the Russian participant at the UNIDIR Cyber Security Conference (Conference "What does a Stable Cyber Environment Look Like?"', UNIDIR, Geneva, 8-9 November 2012) <http://www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf>; Noah Schachtman, 'Darpa Looks to Make Cyberwar Routine With Secret "Plan X"' *Wired* (21 August 2012) <http://www.wired.com/dangerroom/2012/08/plan-x/>.

space).[5] A United Nations Institute for Disarmament Research study of 2011, based on a review of open-source documents, 'identified 33 States [out of 133 States] that include cyber-warfare in their military planning and organisation'.[6] Despite severe deficiencies[7] in the study, it is undeniable that several States have, or are thought to have, such capabilities at their disposal, or are developing them. However, only a very few[8] have issued publicly available cyber security or defence strategies for the military sector, and only one[9] directly addresses offensive cyber activities. In general, States rather emphasise the dependency of the armed forces on the availability, integrity and confidentiality of information and communication systems (ICTs) and thus the aspect of cyber security or defence. Yet, according to a European Defence Agency study of 2013, many States remain at an early level of maturity with regard to the doctrinal and organisational development of their cyber defence (or security) frameworks.[10]

To a certain extent, the 'cyber war' discussion is driven by an overestimation of the scope and consequences of malicious cyber activities, and by an underestimation of the technical expertise and operational sophistication required to launch a 'cyber attack'. The questions of complexity and accessibility of potential target computer systems, e.g., networks supporting critical infrastructure systems are widely disregarded.[11] As most of the current malicious cyber activities are to be categorised as economically or politically motivated cybercrime,

---

[5] eg United States of America, *Department of Defense Strategy for Operating in Cyberspace* (July 2011) 5; The Netherlands, Ministry of Defence, *The Cyber Defence Strategy* (June 2012) 4; Japan, Ministry of Defence, *Toward Stable and Effective Use of Cyberspace* (September 2012) 3.

[6] James A Lewis and Katrina Timlin, 'Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization' (UNIDIR Publication, October 2011) 3 <http://unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf>.

[7] A closer look at the study reveals that States building up, or having at their disposal, cyber security capabilities, eg, Albania, are considered as States 'including cyberwarfare in military planning and organisation', although Albania is in the course of establishing a national "Computer Emergency Response Team" (CERT) with the support of the Carnegie Mellon University, Software Engineering Institute (SEI), and the USAID (development aid agency of the US State Department); see 'SEI grounds Albania-USAID Effort in CERT', Carnegie Mellon University, Software Engineering Institute website <www.sei.cmu.edu/newsitems/rmm-usaid.cfm>. The above was corrected by James A Lewis, 'Cybersecurity and Cyberwarfare: Assessment of National Doctrine and Organisation' in UNIDIR, *The Cyber Index. International Security Trends and Realities* (UNIDIR Publication 2013/3) 9.

[8] These are Russia, the US, the Netherlands and Japan. See Russian Federation, Ministry of Defence, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* (2011, unofficial translation) <http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf> 4ff (see, for example, the definitions of military conflict in information space, information war, information weapons); United States of America (n 5) 5 ('Given its need to ensure the ability to operate effectively in cyberspace and efficiently organize its resources, DoD established U.S. Cyber Command (USCYBERCOM) […]'); The Netherlands (n 5) 11 ('Focal Point 3: Offensive'); Japan (n 5) 4 ('The MOD and SDF [Self Defence Forces] must aim to acquire cutting-edge capabilities in cyberspace just as they do for other domains in order to fulfil its missions such as national defense.').

[9] The Netherlands (n 5).

[10] RAND, 'Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) prepared for the European Defence Agency' (unclassified summary, March 2013) 7.

[11] John B. Sheldon, 'Achieving mutual comprehension: why cyberpower matters to both developed and developing countries' in Kerstin Vignard (ed), *Confronting Cyberconflict* (UNIDIR Disarmament Forum Series 2011/4) 41; Tom Gjelten, 'Is All The Talk About Cyberwarfare Just Hype?' *GBP News* (15 March 2013) <http://www.gpb.org/news/2013/03/15/is-all-the-talk-about-cyberwarfare-just-hype>.

including cyber espionage, scholars caution against an inappropriate militarisation of the topic.[12] Conversely, national security and intelligence advisors,[13] by nature, emphasise the dangers emanating from potential malicious cyber activities. Consequently and understandably, many States believe that, even if by misperception and miscalculation of the risk, malicious cyber activities could result in a conventional, or even nuclear,[14] military conflict.[15]

Discussions of an international agreement to limit the risk of 'cyber conflict' have been conducted at the diplomatic level since the 1990s.[16] In 1998, the Russian Federation proposed for the first time an 'arms-control' treaty that would have banned the use of cyberspace for military purposes.[17] In general, the aim of arms control regimes is to reduce the risk of the outbreak of an (international) armed conflict by reducing the existence or restricting the use of certain weapons.[18] However, for the time being, the majority of experts see little chance of applying traditional arms control regimes to cyberspace.[19]

---

[12] eg Ryan Singel, 'White House Cyber Czar: "There is No Cyberwar"' *Wired Magazine* (4 March 2010) <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>; Myriam Dunn Cavelty, 'The Militarisation of Cyber-space: Why Less May Be Better' in Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012) 141; Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17 Journal of Conflict and Security Law (2) 187, 195-198; Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35 The Journal of Strategic Studies (1) 5.

[13] Especially interesting is the comment on two different threat assessments given by the Director NSA (US) / Commander US CYBERCOM and of the Director of National Intelligence (US) to the US Senate Intelligence Committee, see Gjelten (n 11); cf Jack Goldsmith, 'Cybersecurity Treaties: A Sceptical View' (Stanford University, Hoover Institution, Koret-Taube Task Force on National Security and Law, February 2011) 5 <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf> (Goldsmith is a former US Assistant Attorney General and Special Counsel to the US Department of Defense); Nazli Choucri, *Cyberpolitics in International Relations* (MIT Press 2012) 150ff; Philip Lieberman, 'We're losing the battle against state sponsored attacks' *Help Net Security* (8 April 2013) <http://www.net-security.org/article.php?id=1825>.

[14] cf The President of the United States of America, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (May 2011) 4; United States of America, Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (August 2012) 42; Mark Mazzetti and David E. Sanger, 'Security Leader Says U.S. Would Retaliate Against Cyberattacks' *The New York Times* (12 March 2013) <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all&_r=0>.

[15] James A. Lewis, 'Confidence-building and international agreement in cybersecurity' in Vignard (n 11) 51.

[16] ibid 52.

[17] John Markoff and Andrew E. Kramer, 'U.S. and Russia Differ on a Treaty for Cyberspace' *The New York Times* (27 June 2009) <http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all&_r=0>; Ellen Nakashima, '15 nations agree to start working together to reduce cyberwarfare threat' *Washington Post* (17 July 2010) <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html>; Goldsmith (n 13).

[18] cf Louise Arimatsu, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations' in Czosseck, Ottis and Ziolkowski (n 12) 91, 99.

[19] This opinion is expressed, for example, by the Federal Republic of Germany, 'Cyber security: confidence and security-building measures (CSBMs)', Federal Foreign Office website <http://www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung_/KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html>.

Any endeavour to *reduce the existence of malicious software* would fail, as it is, at present, not practicable and politically feasible to integrate any monitoring and verification mechanism into a treaty. Software is not tangible, is easy to hide, and the mathematical functions or patterns are difficult to recognise as malicious without a thorough and lengthy analysis, and reliable information about the intended use. For example, a code-breaker software could be a dual-use tool, which can be used either for purposes of mending an owned network, or for penetration of a foreign military network. Additionally, it is unlikely that any State would agree to external verification measures requiring scans of all (including classified) governmental computers and diverse data storage devices.[20] Moreover, cyber tools can be produced and employed by non-State actors, in which case, the tools' production would not be subject to any effective regulation.[21] Furthermore, States might not be ready to deprive themselves of the possibilities the cyber tools are offering in terms of a potentially non-lethal, precise means of disruption and interference, e.g., of computer networks of opposing forces during a United Nations (UN) mandated military mission. Finally, the possibilities of acting anonymously within the internet (in the meaning of the technical aspects and physical components of cyberspace) and the challenge of attributing the employment of malicious software would make any legal obligation to reduce its existence futile.

The *restriction of the use* of certain 'cyber weapons' would require a definition of the term which is unfortunately often used in the media and in political[22] and legal science[23] without deliberation. Finding a consensus on a definition of 'cyber weapons' or 'information weapons', focusing either on the means, the aim or the effects of malicious software, must be deemed rather illusory.[24] It should be mentioned that international humanitarian law, as a matter of law and not of political choice, already contains specific limitations on the development and use of certain 'weapons, means or methods of warfare', i.e., including the 'means' of malicious software or the 'method' of employing it.[25]

However, it should also be considered that nuclear and conventional arms control development was historically accompanied by concerns regarding the effectiveness and the

[20] Arimatsu (n 18) 101.

[21] Georg Kerschischnig, *Cyberthreats and International Law* (Eleven International Publishing 2012) 297.

[22] Rex Hughes is predicting the development of a 'new generation' of 'cyber-weaponry' and cyberspace becoming 'ground zero for the next global arms race', see Rex Hughes, 'A treaty for cyberspace' (2010) 86 International Affairs (2) 523.

[23] eg Goldsmith (n 13) 5-7. Kerschischnig defines cyber weapons as 'cyberspace-borne tools and techniques that interfere with a system's normal functioning', whereas the tools 'can be summarized under the term "malware", such as viruses, worms, Trojans, rootkits and botnets, and the techniques would include Dos, infiltration, social engineering, probing, sniffing and mapping', cf Kerschischnig (n 21) 31. Unfortunately, the definition would also apply to cyber tools used by a network administrator for mending their own system.

[24] Arimatsu (n 18) 97ff.

[25] For a thorough analysis, cf ibid 99 and 103-107. Humanitarian Law contains limitations on the development and restrictions of the use of cyber 'means' or 'methods'. It obliges States '[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.' (Article 36 of the Additional Protocol I of 1977 to the Geneva Conventions of 1949).

feasibility of verification and control measures, which have been proven inaccurate over the past decades. Future technological advances could provide feasible (and politically acceptable) verification and control mechanisms for malicious software, although the aspect of skills and knowledge, which plays a crucial role in the intrusion and manipulation of computer networks, could not possibly be covered by verification and control measures.

At present, an arms control treaty for cyber means has, for the above reasons, been deemed not feasible within the international community, so the idea of an international treaty regulating State behaviour in cyberspace has been suggested. On 12 September 2011, China, the Russian Federation, Tajikistan and Uzbekistan proposed, 'in the form of a potential [UN] General Assembly resolution',[26] an *International Code of Conduct for Information Security*.[27] The draft refers, *inter alia,* to non-proliferation of 'information-weapons', stating the obligation of each State:

> '[n]ot to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies' (para. b).

Also in September 2011, the Russian Federation introduced, during an international security conference, another proposal for an international agreement.[28] The *Convention on International Information Security (Concept)*[29] is based on the same guiding principles as the above-mentioned code of conduct, but shows a much higher level of detail, comparable to the 2009 *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation*[30] *on Cooperation in the Field of International Information Security*. The draft concept proposes, *inter alia,* 21 'basic principles for the international information security' (Article 5), several measures aimed at maintaining and fostering international cyber security (Articles 6-12), as well as a set of definitions of terms (Article 2).

[26] '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', UN Doc A/66/359 (14 September 2011).

[27] ibid annex.

[28] The proposal was presented at the 'Ekaterinburg International Meeting of High-Ranking Officials Responsible for Security Matters', hosted by the Russian National Security Council 21-22 September 2011. The draft convention had been elaborated by Russia's National Security Council, the Foreign Ministry and the Moscow State University. cf 'Russia seeks equal cybersecurity for all' *The Voice of Russia* (23 September 2011) <http://english.ruvr.ru/2011/09/23/56634644.html>.

[29] Russian Federation, The Ministry of Foreign Affairs, Convention on International Information Security (Concept), <http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument>.

[30] The Shanghai Cooperation Organisation was founded by The People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan on 15 June 2001.

Although addressing a wide range of cyber threats,[31] neither draft has offered the prospect of forming the basis for negotiations within the international community.[32] Inherent to both proposals is the challenge of finding consensus on the definition of terms such as 'hostile activities' or 'information space'.[33] It should be considered that determining a common cyber terminology, even within a single State, or within international organisations such as NATO, proves to be most difficult. Also, translating definitions into a certain language (e.g., English) does not always reflect the cognitive connotations of wording given within the original mother tongue. Additionally, and adding complexity to the matter, certain terminology (e.g., 'information security', as used by member States of the Shanghai Cooperation Organisation and including the human cognitive domain, versus 'cyber security' as used by many Western States) indicates different approaches with regard to the always necessary balance between security and civil liberties.[34] Some States emphasise the fundamental principle of public international law, namely State sovereignty, as well as States' territorial integrity, political independence, and aspects of national security and political stability. On the other hand, other States underline the importance of universal human rights, support the idea of free flow of information, and promote close international cooperation in law enforcement, including information sharing.[35] Finally, a truly comprehensive regulation of State behaviour in cyberspace would need to include also social and economic aspects, making such an endeavour even more difficult, when considering the political and ideological differences within the international community.

Despite all discrepancies, a common understanding of cyber threats as a global challenge to international peace and security led[36] the international community of States to focus the diplomatic endeavours on a rather practical and (relatively) timely remedy, which does not

[31] Both proposals address the aspects of acts of aggression, cybercrime, terrorist activities, ICT components' supply chain security, and critical infrastructure protection, cf lit b-e of the Draft *International Code of Conduct for Information Security* (n 26), and Article 4 of the *Convention on International Information Security (Concept)* (n 29).

[32] eg William Hague, 'The Rt Hon William Hague MP, London Conference on Cyberspace: Chair's Statement of 2 November 2011', Foreign and Commonwealth Office website <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement> ('Some delegates noted the draft Code of Conduct circulated at the United Nations. There was no appetite at this stage to expend effort on legally-binding international instruments.').

[33] Lewis deems the challenge of finding a common terminology in the cyber arena 'unsolvable', see Lewis (n 15) 53.

[34] cf a thorough analysis by Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in Karlis Podins, Jan Stinissen and Markus Maybaum (eds), *Proceeding of the 5th International Conference of Cyber Conflict* (NATO CCD COE Publication 2013) 413ff.

[35] See detailed discussion in Arimatsu (n 18) 94-97; Lewis (n 15) 55. See also declaration of 32 Western States in UNGA on the importance of universal human rights and free flow of information in cyberspace, *General statement in connection with action on L.30 Developments in the field of information and telecommunications in the context of international security* (6 November 2012) <http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com12/statements/L30_Sweden-joint.pdf>; cf the Swedish approach to the internet as a facilitator of justice, equality and human rights, Government Offices of Sweden, *Enhancing Internet freedom and human rights through responsible business practices,* Sweden, Ministry of Foreign Affairs (13 April 2012) <http://www.government.se/content/1/c6/19/05/60/591bf7d9.pdf>.

[36] According to Lewis, alternatives to a formal cyber treaty began to appear already as early as 2008 (aiming at development of politically binding norms for responsible State behaviour in cyberspace), cf Lewis (n 15) 53.

involve the above-mentioned, highly controversial questions, namely the development of politically binding CBMs for cyberspace.

In the following sections, the concept and cyber-specific aspects of CBMs will be presented (3). Then, the relationship between political and legal commitments will be examined, focusing the importance of political declarations for the interpretation and development of public international law (4). After an overview of international law norms as pertaining to aspects addressed by the sets of adopted, recommended or currently drafted CBMs for cyberspace, these will be analysed as to what extent CBMs can be deemed to reflect or specify State obligations deriving from general principles of public international law (5). Furthermore, the significance of CBMs for NATO will be assessed (6). These sections will be followed by some concluding remarks, which, *inter alia,* will describe the potential significance of CBMs for the interpretation of public international law as it pertains to international peace and security in the context of cyberspace (7).

3. Confidence Building Measures for Cyberspace

CBMs, also known in their advanced forms of 'transparency and confidence building measures' or 'confidence-, transparency- and security-building measures', are an instrument of international politics, negotiated by and applied between States. CBMs aim to prevent the outbreak of an (international) armed conflict by miscalculation or misperception of the risk and by the consequent inappropriate escalation of a crisis situation, by establishing practical measures and processes of (preventive) crisis management between States.[37] In general terms, these measures usually contain aspects of transparency, cooperation, and stability:

- Transparency measures aim to foster a better mutual understanding of national military capabilities and activities. As part of this, crisis management instruments, such as effective crisis communication channels, are usually created and trained; military manoeuvres and movements are notified via diplomatic channels.
- Cooperation measures include exchange of documents (e.g., military doctrines), joint military exercises, exchange of observers, military delegations visits, and development of common understanding of key terms and definitions.
- Stability measures aim to foster predictability of military activities by limitation of them, and through the stabilisation of the military balance.

The notion of CBMs was developed during the Cold War in order to avoid the deployment of nuclear weapons by accident, and have now widened into other areas.[38] Although certain features recur within the international and regional CBMs developed in the context of

[37] cf Zdzislaw Lachowski, 'Confidence-Building Measures' in MPEPIL (n 1) MN 1.

[38] cf United Nations Office for Disarmament Affairs, 'Confidence Building', website <http://www.un.org/disarmament/convarms/infoCBM/>.

specific areas (e.g., outer space) or weaponry, the application of this traditional and established instrument to cyberspace constitutes a complex endeavour.

3.1. Goals, Objectives, Tasks and End-State Desired

The general goals, objectives and tasks of CBMs are described in the preambles of several CBM documents (e.g., the *Final Act of the Helsinki Conference on Security and Co-operation in Europe*[39] of 1975, Part 2). A condensed formulation can be found in the *Guidelines for appropriate types of confidence-building measures and for the implementation of such measures on a global or regional level*, prepared by the UN Disarmament Commission's Consultation Group in 1988.[40] According to these guidelines:[41]

- '[t]he **ultimate goal** of confidence-building measures is to strengthen international peace and security and to contribute to the prevention of all wars [...]';
- '[a] **major objective** is to reduce and even eliminate the causes of mistrust, fear, misunderstanding and miscalculations with regard to relevant military activities and intentions of other States […]';
- '[a] **centrally important task** [...] is to reduce the danger of misunderstanding or miscalculation of military activities, to help to prevent military confrontation as well as covert preparations for the commencement of a war, to reduce risk of surprise attacks and of the outbreak of war by accident; and thereby, finally, […] to enhance security and stability.'

Although being drafted in the context of disarmament, the guidelines depict CBMs in a general way as suitable for deliberations on CBMs for cyberspace. Overall, CBMs aim at reaching a sufficient level of predictability of State behaviour at the international level, and to prevent 'loss of control' over a situation in terms of escalation. Consequently, the ultimate end-state desired of CBMs for cyberspace can be described as:

- a common understanding of acceptable State behaviour in cyberspace, and
- a state of cyber stability in international relations.

[39] *The Final Act of the Conference on Security and Cooperation in Europe* (1 August 1975) (Helsinki Declaration), Part 2: *Document on confidence-building measures and certain aspects of security and disarmament*, (1978) 14 ILM 1292.

[40] UNGA, *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament,* UN Doc A/S-15/3 (28 May 1988) 28-33 (endorsed by UNGA Res 43/78H, 7 December 1988).

[41] ibid 30 (para 2.2.1.), 31 (para 2.2.5. and 2.2.6.) [emphasis by the author].

Importantly, CBMs for cyberspace cannot respond to all cyber threats as relevant to national cyber security, which, according to most national cyber security strategies,[42] would also include aspects of economically or politically motivated cybercrime (including cyber espionage) conducted by both States and non-State actors. CBMs do not aim to present a kind of 'international cyber security strategy' (although some aspects usually addressed in national strategies, e.g., law enforcement, are also partly considered in the course of current CBMs negotiations) and to improve the global cyber security. CBMs address specifically the level of inter-State relations and aim primarily at the prevention of an outbreak of an (international) armed conflict because of misunderstanding and miscalculation of risk.

Indeed, the danger of misunderstanding or miscalculating the intentions or activities of States is particularly increased in the context of cyberspace, due to the specific characteristics of the internet. As malicious cyber activities are not immediately 'visible' in the usual meaning of the term and are not easily attributable to a specific perpetrator, ambiguity, doubt and suspicion are likely to govern international relations. Therefore, and even more so than in other areas of military activities, risk reduction and stabilisation concerning governmental activities are of the utmost importance for the maintenance of international peace and security. As traditional and proven means of risk reduction and stabilisation by deterrence (through the possibility of retaliation) are not feasible[43] in cyberspace due to the challenge of attribution, tools of preventive diplomacy such as CBMs seem to be a viable solution.

3.2. Challenges of Cyberspace

In the past, CBMs have taken a formal or informal, legal or political, unilateral, bilateral, regional or multilateral nature. With regard to content, they range from establishing hotline-communication lines, through unilateral declarations of no first use of certain weaponry, to legally binding arms control treaties with sophisticated verification and control mechanisms. Thus, the CBM concept shows a high level of elasticity. However, its application to cyberspace is a challenging endeavour. A dedicated study, as elaborated[44] by a UN Governmental Group of Experts (GGE)[45] with regard to another 'space' driven by specific characteristics of technology, namely outer space,[46] is yet to be conducted. With regard to the contents, CBMs for cyberspace surely cannot merely replicate the existing sets of

[42] eg OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* (2012, OECD Digital Economy Papers 211) 5 <http://dx.doi.org/10.1787/5k8zq92vdgtl-en>.

[43] cf Eric Sterner, 'Retaliatory Deterrence in Cyberspace' (2001) 5 Strategic Studies Quarterly (1) 66; contra: The President of the United States of America (n 14); Forrest Hare, 'The Significance of Attribution to Cyberspace Coercion: A Political Perspective' in Czosseck, Ottis and Ziolkowski (n 12) 125, 135ff.

[44] *Prevention of an Arms Race in Outer Space: Study on the Application of Confidence-Building Measures in Outer Space*, UNGA Res 48/305 (15 October 1993).

[45] UNGA Res 45/55B (4 December 1990).

[46] cf Andrey Makarov, 'Transparency and Confidence-Building Measures: Their Place and Role in Space Security' in UNIDIR, *Security in Space* (The Next Generation-Conference Report, 31 March – 1 April 2008) <http://unidir.org/pdf/articles/pdf-art2817.pdf>.

measures developed for nuclear, conventional and other weapons, the detailed presentation of which would certainly exceed the scope of this paper.[47]

Hitherto, the significance of CBMs has been acknowledged in the context of disarmament and arms control.[48] CBMs were particularly meant[49] for facilitating the adoption of disarmament or arms control measures, being thus merely a means to an end. Accordingly, some international treaties contain CBMs.[50] As disarmament or arms control commitments are not feasible with regard to cyberspace (para. 2), CBMs for cyberspace cannot be regarded as a means to achieve this end. They must show significance *per se* and present a self-contained (preventive) crisis management mechanism.

Furthermore, CBMs in the traditional disarmament and arms control arena were developed in an environment where States mostly held the monopoly of use of force and were in possession of the majority of the weaponry and other military means relevant to international peace and security. As the capabilities and knowledge necessary for conducting significant malicious cyber activities are globally widespread – also outside the governmental sector –, the initial situation for the development of CBMs for cyberspace is very different. At first sight, this statement could be countered by the existence of arms control regimes (namely measures against illicit trade) for light arms and small weapons,[51] which can also be often found in hands of non-State actors. However, the main difference to light arms and small weapons is that States cannot control the production and the quantity of malicious software. Thus, also in this regard, the situation for development of CBMs for cyberspace shows dissimilar features.

For reasons expressed above (para. 2), CBMs referring only to the reduction of the existence or limitation of the use of certain weaponry cannot serve as an appropriate scheme for CBMs for cyberspace. In the context of CBMs referring to *specific weaponry*, at first sight, only the traditional[52] CBM regarding the exchange of information on military spending seems transferable. However, offensive cyber capabilities are characterised rather by skills than by the equipment purchased. In the cyber context, this feature minimises the importance of 'military spending', otherwise a significant indicator for the defensive or offensive orientation of a State, as expenditure on the training of hackers is not comparable with the spend on conventional or other armaments. Furthermore, declaring 'military spending' would need to include both funds spent on the development and maintenance of (passive) defensive cyber capabilities and the funds spent on (active) offensive cyber

[47] cf Lachowski (n 37), as well as on respective websites of the UN Office of Disarmament Affairs (n 38), OSCE <http://www.osce.org/fsc/44569>, and OAS <http://www.oas.org/csh/english/csbm.asp>.

[48] eg UNGA Res 59/92 (17 December 2004) preamble.

[49] cf n 40.

[50] cf Lachowski (n 37) 5.

[51] cf UN Office for Disarmament Affairs endeavours with regard to 'Firearms Protocol', 'Programme of Action on small arms - including an Instrument on marking and tracing', and 'Basic Principles on the Use of Force and Firearms by Law Enforcement Officials', <http://www.un.org/disarmament/convarms/SALW/>.

[52] cf UN Office for Disarmament Affairs (n 38).

capabilities, leaving such a declaration meaningless in terms of indication of defensive or offensive orientation of a State's military. A respective separation of funds would not be reasonable as, for example, funds spent on the education of military personnel with regard to current hacking methods can be classified as both, in that it is used to conduct offensive operations and for (passive) cyber defence measures in terms of acquiring knowledge necessary for improvement of the resilience of their own network.

Also, any CBMs referring to geographical areas, for example, agreements on demilitarised zones are not feasible in the context of cyberspace, due to its global scope. The same applies to operational measures, such as the limitations of military manoeuvres and exercises, due to the possibility of operating covertly in cyberspace. As mentioned above (para. 2), also any traditional CBMs requiring verification and control are not suitable.

However, CBMs referring to information sharing and cooperation could serve as a suitable model for measures for cyberspace. A detailed listing of such CBMs was elaborated by the Organisation of American States (OAS) Permanent Council (Committee on Hemispheric Security). The *Consolidated List of Confidence and Security Building Measures*[53] includes 36 such measures (based on three political declarations by the OAS member States).[54] They refer, *inter alia,* to general cooperation commitments, which would potentially be suitable for adaption in cyberspace, such as:

- exchange of information on the organisation, structure, size and composition of defence and security forces,
- advance notice of military exercises,
- conduct of joint training and exercises between armed forces, and
- defence visit programmes with regard to installations.

If 'translated' to cyberspace, such measures would include:

- exchange of information on the organisation, structure, size, and composition of computer network operations (CNO) units,
- advance notice of live hacking exercises by CNO units,
- conduct of joint training and exercises between CNO units, and

[53] OAS, Permanent Council, Committee on Hemispheric Security, *Consolidated List of Confidence and Security Building Measures for Reporting according to OAS Resolutions* (Approved at the meeting of 15 January 2009) <http://www.oas.org/csh/english/csbmlist.asp#Santiago>.

[54] OAS, *Declaration of Santiago on Confidence- and Security-Building Measures* (10 November 1995, OEA/Ser.K/XXIX.2, COSEGRE/doc.18/95 rev 3); *Declaration of San Salvador on Confidence- and Security-Building Measures* (28 February 1998, OEA/Ser.K/XXIX.2, COSEGRE.II/doc.7/98 rev 3); *Declaration by the Experts on Confidence- and Security-Building Measures: Recommendations to the Summit-Mandated Special Conference on Security* (4 February 2003, OEA/Ser.K/XXIX, RESEGRE/doc.4/03 rev 3).

- visits of CNO units and their computer laboratories.

Such measures would, most probably, be difficult to implement in the cyber context because of the unwillingness of States to disclose in detail the level of sophistication of their offensive cyber forces, and of the knowledge and abilities of the respective personnel. However, the OAS list contains other measures, which could be of value for cyberspace, such as:

- exchange of defence policy and doctrine papers,
- establishment of national points of contact regarding critical infrastructure protection,
- exchange information on scientific research, and
- exchange of contacts between students, academics, and experts in defence and security studies.

Another example of comprehensive CBMs is the series of documents developed by the Organization for Security and Co-operation in Europe (OSCE) (the organisation's Forum for Security Co-operation) since 1975. The most recent OSCE CBM document is the *Vienna 2011 Document on Confidence- and Security-Building Measures (CSBMs),*[55] which presents a politically binding commitment from all 57 member States[56] from Europe, Central Asia and North America. Also, this set of CBMs considers, apart from measures relating to weaponry, verification and control, extended information sharing and cooperation measures, comparable to the aforementioned CBMs developed by the OAS.

Thus, CBMs for cyberspace could contain some of the cooperation and information sharing measures as endorsed in existing political commitments referring to non-cyber-specific areas. Additionally, CBMs in form of political declarations, as also contained in traditional disarmament and arms control regimes (e.g., declarations on 'no first use'), are viable in the cyber context. It could, however, prove beneficial to conduct an in-depth analysis of 'lessons identified' as collected during the last decades by armed forces and peace research institutes with regard to nuclear and conventional arms control regimes, in order to consider the general findings during the negotiations of CBMs for cyberspace.

3.3. Current Developments and Proposed Contents

The endeavours to develop CBMs for cyberspace are mainly taking place within the fora of the UN (3.3.1.) and the OSCE (3.3.2.). Respective negotiations conducted within the regional

[55] OSCE, *Vienna 2011 Document on Confidence- and Security-Building Measures (CSBMs)*, Doc No FSC.DOC/1/11 (30 November 2011).

[56] idem, 'What is the OSCE?', Factsheet <http://www.osce.org/secretariat/35775>; idem, 'Who We Are', OSCE website <http://www.osce.org/who>.

organisation Association of South East Asian Nations (ASEAN)[57] and the informal group G8[58] cannot be presented due to lack of publicly available information. Furthermore, CBMs are negotiated at a bilateral level (3.3.3.). Also, some States have issued unilateral declarations, which show their views on politically acceptable contents of CBMs for cyberspace (3.3.4.).

3.3.1. UN

Cyber security entered the UN agenda in 1998, when the Russian Federation first introduced a draft resolution titled *Developments in the field of information and telecommunications in the context of international security*[59] in the First Committee of the UN General Assembly (UNGA). Since then, two principal 'streams' can be identified with regard to the work of the UN in the arena of cyber security:

1. the politico-military stream within the UNGA First[60] Committee (Disarmament and International Security), focusing on international security in cyberspace, and
2. the economic stream focusing on infrastructure protection and cybercrime within the UNGA Second[61] (Economic and Financial) Committee and, to a certain extent, within the Third[62] (Social, Humanitarian and Cultural) Committee.[63]

---

[57] ASEAN, *Chairman's Statement of the 19th ASEAN Regional Forum Phnom Penh, Cambodia* (12 July 2012) 5 <http://aseanregionalforum.asean.org/library/arf-chairmans-statements-and-reports.html>.

[58] cf Federal Republic of Germany (n 19); G8, *Deauville G8 Declaration, Renewed Commitment for Freedom and Democracy* (26-27 May 2011, Deauville, France) para 5 <http://ec.europa.eu/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf>.

[59] UNGA Res 53/70 (4 December 1998) (adopted without vote).

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

[61] cf *Creation of a global culture of cybersecurity,* UNGA Res 57/239 (20 December 2002) (proposing nine elements for creating a global culture of cybersecurity, annex), *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* UNGA Res 58/199 (23 December 2003) (proposing eleven elements for protecting critical information infrastructures, annex), and *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, UNGA Res 64/211 (21 December 2009) (proposing 'voluntary self-assessment tool for national efforts to protect critical information infrastructure' of 18 points, annex).

[62] cf UNGA Res 55/63 (4 December 2000) and 56/121 (19 December 2001) (combating the criminal misuse of information technologies), 57/239 (20 December 2002) (creation of a global culture of cybersecurity) and 58/199 (23 December 2003) (creation of a global culture of cybersecurity and the protection of critical information infrastructures), 64/211 (21 December 2009) (creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures), 55/63 (22 January 2001) and 56/121 (23 January 2002) (combating the criminal misuse of information technologies), and UNGA Res 63/195 (18 December 2008), 64/179 (18 December 2009), and 65/232 (21 December 2011) (strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular, its technical cooperation capacity). The Third Committee deferred considerations on the subject on the criminal misuse of information technologies, pending work of the Commission on Crime Prevention and Criminal Justice, UNGA Res 56/121 (23 January 2002, para 3).

Since 2004, all in all, six GGEs on cyber-related issues were established within the UN framework, *inter alia,* on identity-related crime (established in 2004 by the UN's Economic and Social Council), the development of a cyber security agenda (established by the International Telecommunication Union (ITU) in 2007), and on cybercrime in general (open-ended GGE established by the United Nations Office on Drugs and Crime in 2010).[64] Within the area of responsibility of the First Committee, upon a proposal of the Russian Federation of 2001, a Group of Governmental Experts on Developments in the Field of Information and Communications in the Context of International Security was convened to discuss the threats, possible cooperation and other issues of international information security. This GGE[65] (2004-2005) failed to reach a consensus and to submit a report. It was followed by a second GGE[66] (2009-2010), which was able to reach an agreement on recommendations for future actions, including the development of CBMs:[67]

> '[T]he Group of Governmental Experts considers it useful to recommend further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions: [...]
> (ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict,
> (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices; [...]
> (v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.' [68]

A third GGE (2012-2013) was established 'to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including [...] confidence-building measures with regard to information space […].'[69] The group reached consensus and issued a report on 7 June 2013. It includes the following recommendations on CBMs for cyberspace:[70]

---

[63] For detailed information see Tim Maurer, 'Cyber Norm Emergence at the United Nations. An Analysis of the Activities at the UN Regarding Cyber-Security' (Harvard University, John F. Kennedy School of Government, Belfer Center for Science and International Affairs, Discussion Paper No. 2011-11, September 2011) 20-45.

[64] ibid 18.

[65] Established upon UNGA Res 58/32 (8 December 2003) para 4.

[66] Established upon UNGA Res 60/45 (8 December 2005) para 4.

[67] UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (16 July 2010) UN Doc A/65/201 (30 July 2010) 8, para 18.

[68] ibid.

[69] UNGA Res 66/24 (13 December 2011) ibid para 4.

[70] UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (7 June 2013) UN Doc A/68/98 (24 June 2013, reissued for technical reasons on 30 July 2013) para 26.

- voluntary exchange of views and information on national strategies and policies, best practices, decision-making processes, relevant national organisations, and measures to improve international cooperation,
- creation of bilateral, regional and multilateral consultative frameworks for confidence building, e.g., workshops, seminars, and exercises,
- expanded information sharing on ICT security incidents,
- exchanging names and contact information of national points of contact for crisis management, including Computer Emergency Response Teams (CERTs),
- increased cooperation to address security incidents that could affect ICT infrastructures or critical infrastructure, and
- enhanced mechanisms for law enforcement cooperation (with regard to incidents that could otherwise be misinterpreted as hostile State actions).

The report uses the term 'ICT', thus avoiding the controversial terms 'cyberspace' *versus* 'information space', which both include contentious political connotations (section 2). Content-wise, the GGE recommendations address a wide range of cyber threats, including cyber crime and critical infrastructure security (earlier drafts went even further, referring to law enforcement in general and to expanded cooperation on combating the use of ICTs for terrorist purposes). Thus, the CBMs proposal extends beyond the traditional notion of CBMs as a tool of prevention of the outbreak of an international armed conflict (section 3.1) and resembles rather a draft of an 'international cyber security strategy' (under the disguise of CBMs). It therefore appears ambitious which, at the same time, may challenge the adoption of the proposed CBMs at a wider international level, beyond the 15[71] States participating in the group. It should be mentioned that the abstract references to cooperation ('increased cooperation', 'enhanced mechanisms') without formulation of specific (confidence building) measures could minimise the significance and practical impact of the proposed CBMs. In contrast to the recommendation of the second GGE, 'finding possibilities to elaborate common terms and definitions' with regard to ICT security was not attempted.

3.3.2. OSCE

The OSCE is an organisation with a considerable experience and a successful history with regard to the development of CBMs in the conventional weapons area. Since 2011, the OSCE has shown a comprehensive[72] approach to cyber security, having previously focused its activities on individual aspects[73] of cyber security, such as combating cybercrime and the use

[71] The GGE consists of members from Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, the UK and the US, cf United Nations Office for Disarmament Affairs website <http://www.un.org/disarmament/topics/informationsecurity/>.

[72] OSCE, *Resolution on the Overall Approach of the OSCE to Promoting Cybersecurity* in OSCE, *Resolutions of the OSCE Parliamentary Assembly Adopted at the Twentieth Annual Session, Belgrade, 6 to 10 July 2011* (Doc No AS (11) R E) 18ff.

[73] OSCE, 'Cyber security: virtual threats, real responses', website <http://www.osce.org/home/76011>.

of the internet for terrorist purposes. On 26 April 2012, following a respective resolution of the Parliamentary Assembly of 2011,[74] the OSCE Permanent Council established an open-ended, informal working group under the auspices of the organisation's Security Committee '[t]o elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs'.[75]

According to a document of November 2012 and the last draft version of 31 May 2013, the CBMs for cyberspace discussed during the process included, for example:[76]

- voluntary exchange of national views on aspects of national and international threats to ICT [this could include views on relevant doctrines, strategies, norms, lessons learned, concepts for operating in cyberspace],
- voluntary information sharing, e.g., about national organisations, programmes, or strategies relevant to ICT security,
- voluntary consultations, in order to reduce risk of conflict resulting from the use of ICT,
- voluntary provision and annual updating of contact data of existing national structures which manage ICT-related incidents and coordinate responses [this could include CERTs but also at the organisational and political level],
- voluntary establishment of measures to ensure rapid communication at policy levels of authority [i.e., communication-hotlines between capitals],
- voluntary provision of a list of national terminology relating to ICT security accompanied by explanation or definitions of the terms, and
- voluntary exchange of views as to how to use existing OSCE mechanisms to facilitate communication regarding incidents involving ICT.

The approach of the informal working group, assessed solely on the basis of the aforementioned documents, shows hopeful prospects for a successful accomplishment of the task. The set of CBMs uses the term 'ICT', avoiding the controversial terms 'cyberspace' *versus* 'information space'. Additionally, it strongly focuses on transparency measures and avoids the aspects of cooperation measures going beyond hotline communications in cases of incidents or consultation, such as enhanced cooperation in law enforcement, which is approached with caution by those States which emphasise the aspect of State sovereignty

[74] idem (n 72) 19, para 11.

[75] idem, Permanent Council, *Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (Decision No. 1039, Doc No. PC.DEC/1039, 26 April 2012).

[76] See United States Mission to the OSCE, *Informal Working Group Established by PC Decision 1039: Revised Draft Set of CBMs* (Doc No PC.DEL/871/Rev.1, 7 November 2012) <http://www.par-anoia.net/assessment/at/OSCE_Reprise/pcdel0871r1%20usa%2c%20draft%20set%20cbms.pdf> (document shared by Anonymous 'intelligence agency' Par:AnoIA). The draft version of 31 May 2013 is not publicly available. Additions in brackets are those of the author.

(and consequently territorial jurisdiction) in cyberspace. Last but not least, the OSCE approach is based not only on a notion of CBMs as a political commitment of States, but leaves the States a broad freedom of decision, affirming all proposed specific CBMs to be 'voluntary'. It was hoped that consensus on a set of CBMs for cyberspace could be reached by the group in 2012.[77] The results are still awaited.

3.3.3. Bilateral Endeavours

The US and Russia had already entered into discussions about internet security in 2009.[78] According to a joint statement of the Presidents of the US and of Russia, a bilateral agreement on CBMs for cyberspace was concluded between the States in June 2013.[79] It includes:[80]

- establishment of a communication channel and information-sharing arrangements between CERTs (for protection of critical information systems),
- authorisation of the use of the direct communications link between the States' Nuclear Risk Reduction Centers (exchange of urgent communications employing around-the-clock staffing at the Department of State in Washington, D.C., and the Ministry of Defense in Moscow),
- establishment of a direct secure voice communications line between the US Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council (to manage potentially dangerous situations arising from events that may carry security threats to, or in the use of, ICTs), and
- creation (within a month) of a bilateral working group on issues of threats to, or in the use of, ICTs in the context of international security (in the framework of the US-Russia Bilateral Presidential Commission).

The exchange of strategic documents and of 'military views on cyberspace operations', which was foreseen during the negotiations, according to an intermediate joint statement[81] of the Parties of 2011, is not included in the set of CBMs, as the Parties exchanged earlier

[77] OSCE, Permanent Council (n 75).

[78] John Markoff and Andrew E. Kramer, 'In Shift, U.S. Talks to Russia on Internet Security' *The New York Times* (12 December 2009) <http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0>.

[79] The White House, *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building* (17 June 2013) <http://www.whitehouse.gov/the-press-office/2013/06/17/joint-statement-on-a-new-field-of-cooperation-in-confidence-building>.

[80] ibid; The White House, *U.S.-Russian Cooperation on Information and Communications Technology Security,* Factsheet (17 June 2013) <http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>.

[81] idem, *Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin, U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace* (23 June 2011) <http://www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf>;

white papers and unclassified military ICT strategies and other relevant studies.[82] The CBMs focus on information exchange at high political and technical (tactical) levels in crisis situations. Hereby, the information exchange could also include, for example, warnings with regard to cyber exercises that might be misperceived as threats.[83] The creation of the working group indicates the prospect of further dialogue on cyber security. The involvement of communication channels at high political levels underlines the importance of the topic for the two States and could support the effective implementation of the agreement.

Talks on cyber security between the US and China are also probably being conducted, as indicated by a Chinese proposal reported in March 2013.[84] Between 2009 and June 2012, the US-based Center for Strategic and International Studies and the China Institute of Contemporary International Relations have held six formal meetings on cyber security (accompanied by several informal discussions), called *Sino-U.S. Cybersecurity Dialogue*. The meetings have been attended, beside academics, by a broad range of US and Chinese officials. The goals of the discussions have been, among others, to identify areas of potential cooperation, including CBMs.[85] The content of the discussion series resembles preparations for an official CBMs negotiations process.

3.3.4. Unilateral Declarations

Furthermore, some States have issued unilateral declarations, expressing their views on the possible content of CBMs for cyberspace.

Germany's proposal for CBMs for cyberspace, as posted on the website of the Federal Foreign Office, includes the following key elements:[86]

- transparency measures:
    - exchange of information on applicable international law, on organisational structures, strategies and contact partners,
    - exchange of white papers on military organisations and, where available, doctrines in the cyber sphere, and
    - risk reduction.

[82] idem, Factsheet (n 80).

[83] Ellen Nakashima, 'U.S. and Russia sign pact to create communication link on cyber security' *The Washington Post* (17 June 2013) <http://articles.washingtonpost.com/2013-06-17/world/40025979_1_cyber-security-pact-homeland-security>.

[84] Terril Yue Jones, 'China says willing to discuss cyber security with the U.S.' *Reuters* (12 March 2013) <http://www.reuters.com/article/2013/03/12/us-usa-china-cybersecurity-idUSBRE92A0XO20130312>.

[85] China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS), *Joint Statement. Bilateral Discussions on Cooperation in Cybersecurity* (June 2012) 1 <http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf>.

[86] Federal Republic of Germany (n 19).

- stability measures:
    - establishment or consolidation of crisis communication channels,
    - establishment of CERTs and necessary procedures for exchange, and
    - joint cyber exercises.

More detailed sets of CBMs were issued by the Russian Federation. The *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* of 2011 commits the armed forces to support [the Russian Federation in] the development of CBMs in the sphere of the military use of information space. The measures proposed in the document include:[87]

- exchange of national concepts for ensuring security in the information space,
- timely exchange of information regarding crisis events and threats in the information space and measures taken with respect to their settlement and neutralisation, and
- consultations on the issues of activity in the information space, which may cause the parties' concern, and the cooperation regarding the settlement of any conflict situations of military character.

The focus point here is on the (voluntary) information exchange necessary for actual, preventive and even precautionary crisis management, and on consultation (referring to concepts securing cyber security, information exchange concerning cyber threats and respective measures to their settlement and neutralisation). During a conference in 2012, a Russian representative presented a longer list of potential CBMs, adding to the aforementioned list the following aspects not specific to the armed forces:[88]

- harmonisation of national legislation in order to ensure information safety,
- elaboration of a universal glossary of international information security terms, and
- development of a system of international cooperation among law enforcement agencies with a view to preventing crime in the information sphere.

This longer list of possible CBMs for cyberspace not only indicates an approach towards Russia's Western negotiation partners, e.g., concerning law enforcement cooperation, but also exceeds all expectations by proposing 'harmonisation of national legislation' with regard to cyber security; a proposal which is very ambitious. Additionally, the proposal to elaborate a universal glossary of ICT terms reflects the recommendation of the second GGE of 2010 (para. 3.3.1.).

[87] Russian Federation (n 8) 12ff.

[88] Fedosov (n 4).

3.3.5. Assessment

All in all, a comparison of the above-mentioned sets of CBMs for cyberspace with a list of 'traditional' CBMs, as developed, say, within OSCE or OAS in the context of traditional disarmament and arms control, clearly shows that CBMs for cyberspace, as currently discussed, present a minimum of possible political commitments. It reflects the level of controversy surrounding governmental cyber activities, and might additionally be affected by the different levels of sophistication of States with regard to the development of cyber infrastructure, the governmental use of ICT, and the national cyber security framework in terms of, for example, the existence of telecommunication regulations and other relevant legislation, cyber crisis management mechanisms, or the existence of a governmental or national CERT.

However, there might be a value in the elaboration of the first CBMs for cyberspace, which can serve as a basis for future developments in that arena. It should be mentioned that, surprisingly, the current developments of CBMs for cyberspace, as far as respective documents are publicly available, do not contain any reference to a CBM of exchange of scientific research or of academic personnel (as, e.g., endorsed in the OAS-CBMs), a measure, which could be considered as politically rather innocuous.

3.4. Nature of the Commitments

The nature of potential CBMs for cyberspace as political commitment and their geographical scope are both predisposed by the unique characteristics of the internet.

3.4.1. Politically Binding versus Legally Binding

As mentioned above (para. 2), due to political and ideological differences within the international community, there is little prospect for a comprehensive, legally binding regime for cyberspace. CBMs, on the contrary, require an agreement on process rather than on values, and therefore present a more realistic approach to creating an international framework for State behaviour in cyberspace.[89] As mentioned above (para. 3.2.), CBMs can have a nature of either a political commitment or a legally binding obligation; the latter endorsed within specific arms control treaties, or in specific crisis prevention agreements[90] for the military sector. However, for the following reasons, legally binding CBMs are not feasible in the context of cyberspace.

[89] cf Lewis (n 15) 59.

[90] eg *Agreement On The Prevention Of Dangerous Military Activities* concluded between the US and the USSR on 12 June 1989 (in force since 1 January 1990, 1566 UNTS, Reg No. I-27309) and between Canada and USSR on 10 May 1991 (in force since 10 November 1991, 1852 UNTS Reg No. I-31540), or *Agreement on the Prevention of Incidents On and Over the Waters Outside the Limits of the Territorial Sea of 25 May 1972, As Amended by the 1973 Protocol to the Agreement and the 1998 Exchange of Diplomatic Notes* between the US and the USSR (all in force with the successor Russian Federation).

The value of legal obligations of States in international relations is, *inter alia,* the possibility to 'retaliate' for the breach of said obligations in a legal manner by recourse to countermeasures (i.e., otherwise illegal acts undertaken in response to a previous intentional wrongful act of another State),[91] to the jurisdiction of the International Court of Justice (ICJ) or of (*ad hoc*) arbitration tribunals. Such legal remedies, however, require a clear attribution of the act which is supposed to breach the legal obligation in question, to a State. In the context of cyberspace, questions of attribution, and thus of State responsibility, should be based on a threefold concept, including (1) technical, (2) legal and (3) political aspects:

(1) Due to diverse technical possibilities, the attribution of malicious cyber activities of a sophisticated nature to a specific IT-system will, despite contrary allegations, as for example, by the recent Mandiant APT1 report,[92] most often be difficult, if not impossible. Hackers predominantly act anonymously, e.g., by choosing a multitude of different and complex routes for their Internet Protocol (IP) addresses[93] and other technical information[94] the computer sends during an internet session. Additionally, the malicious data stream can be encrypted and conducted through a chain of numerous computers belonging to innocent individuals, showing one of them as the source of the malicious activities. Thus, even after an extensive forensic analysis of the malicious data stream, the identification of the computer system the activities originated from, and pinpointing its geographical location, can seldom be affirmed with utmost certainty.

(2) The legal attribution is based upon the technical attribution. Even if the technical attribution could affirm a specific computer system as the one from which the malicious cyber activities originated, the legal attribution would require evidence

[91] eg Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press 1963) 281ff.

[92] The report of the US-based information security company Mandiant of February 2013 claims the attribution of malicious cyber activities conducted against IT systems and computer networks based in the US to China's government. The report was widely criticised within the cyber security community for its analytic flaws and 'expectation bias'. See *Mandiant, APT1 – Exposing One of China's Espionage Units* (Report, February 2013) <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>; see critical analysis, eg, Jeffrey Carr, 'Mandiant APT1 Report Has Analytical Flaws', blog (19 February 2013) <http://jeffreycarr.blogspot.com/2013/02/mandint-apt1-report-has-critical.html>.

[93] An IP address (Internet Protocol number) is a 12 digit number identifying a computer or other network device during an internet session. An IP data package is the basic element of data transmission via the internet. It comprises of a header (information on the source, destination, status and fragmentation of the transmitted data) and a payload (transmitted data).

[94] eg Media Access Control address or Airport ID for Apple operating systems (order of numbers identifying hardware); Address Resolution Protocol (assignment of a MAC address or Airport ID to an IP address); Service Set Identity (network name); Wired Equivalent Privacy Protocol (coded details about the network); as well as details on the adjustments of the operating system. These details are, if not blocked, automatically transferred during the internet session to any computer requesting this information by a so-called PING (Packet InterNet Grouper). A PING is computer software sending an ICMP-Echo-Request data package to the destination address of the host which is to be scanned, i.e., to the IP address, to the Domain Name System name (DNS name) or to the Network Basic Input Output System name (NetBIOS name) of the targeted computer. The targeted system automatically responds by an ICMP-Echo-Reply if, according to the usual adjustments of the system, the system supports the ICMP package.

(i.e., reliable and unclassified intelligence) about the person or persons involved in the preparation and/or conduct of the activities in question, and about their relationship to a State. The latter, in general terms, would imply that the persons acting were State organs (or otherwise exercising State authority), or acting, 'on the instructions of, or under the direction or control of' a State (see Articles 4-11 of the *Draft Articles on Responsibility of States for Internationally Wrongful Acts*[95] of the International Law Commission (ILC)). It should be mentioned that the issue of State responsibility is a subject of judicial and scholarly controversy (especially with regard to the question whether 'control' is to be deemed as 'overall' or 'effective' control) and respective information on such matters presenting clear evidence is surely not easy to obtain.

As a general rule, international judges have wide-ranging discretion in the assessment of evidence (principle of free assessment of evidence).[96] Although international courts and tribunals do employ[97] 'presumptions of fact' as an established tool of legal reasoning (not evidence), and the standard of *prima facie*[98] as evidence, legal attribution based solely on the context ('suggestive evidence', 'circumstantial evidence' or 'indication') is not sufficient within the context of attribution in legal terms. This was confirmed by the jurisprudence of the ICJ in the cases *Nicaragua*[99] and *Oil Platforms.*[100] Thus, for example, an analysis of 'behaviour-based algorithms', as partly claimed[101] to support the identification of the originator of malicious cyber activities, is to be deemed as a mere indication (of a rather weak nature), as behavioural patterns (or 'hacking techniques') as used in certain geographical regions by governmental intelligence agencies, for instance, can be imitated in order to intentionally provide a misleading trail.

All in all, despite the interdependency between public international law and international politics, international law contains evidentiary rules, which cannot be replaced by political considerations, indications ('circumstantial attribution') or by suspicions.

(3) Political attribution displays, in a way, less strict standards, offering the possibility to interpret malicious cyber activities in the context of the overall political

[95] UNGA Res 56/83 (12 December 2001) annex.

[96] *Military and Paramilitary Activities in and against Nicaragua,* Merits (1986) ICJ Rep 14, para 60 ('[...] within the limits of its Statute and Rules, it [the ICJ] has freedom in estimating the value of the various elements of evidence.').

[97] Rüdiger Wolfrum, 'International Courts and Tribunals, Evidence' in MPEPIL (n 1) MN 67.

[98] ibid 78.

[99] *Nicaragua* (n 96) 109 ('Yet despite the heavy subsidies and other support provided to them by the United States, there is **no clear evidence** of the United States having actually exercised such a degree of control in all fields so as to justify treating the *contras* as acting on its behalf.' [emphasis by the author]).

[100] *Oil Platforms,* Merits, (2003) ICJ Rep 161, para 59.

[101] eg US Department of Defense, *Cyberspace Policy Report,* Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 (November 2011) 4.

situation, and to make use of concepts such as the *cui bono* test. Such an attribution would surely need to be based on a thorough political analysis, going beyond mere suspicions and the usual concept of 'the enemy'. However, political attribution alone, being 'circumstantial', would certainly be not sufficient in the context of attribution of a treaty breach or other internationally wrongful act to a State in the context of international law, although it presents a perfectly sufficient basis for carrying out political and diplomatic remedies.

The attribution of a treaty breach or an otherwise internationally wrongful act to a State would require proof of technical and legal attribution, whereas the political attribution could serve as a supporting argument only. The lack of technical and legal attribution of malicious cyber activities to a State, which, in practice, is highly probable, will make any allegation of a treaty violation impossible, and thus any treaty-based obligation futile. To quote a grand lawyer: 'Anonymity is a norm destroyer'.[102] Political imputation, based on circumstances and indices, bears the risk of misjudgement, misinterpretation and thereby inappropriate escalation; aspects that CBMs aim to prevent (para. 3.1.).

It should be mentioned that the lack of attribution or evidence establishing State responsibility is not a new challenge to public international law. In the context of international environmental law, the natural environment being another global resource like the internet, pollution can spread across State borders without (immediate) attribution of the source of the contamination. As a reaction to this, the customary principles of prevention and precaution, including early warning, (*post factum*) information-sharing, etc., were developed.[103] Several of those principles are also aspects considered in the negotiations of CBMs for cyberspace.

A further argument supporting the development of CBMs as political commitments is of a rather practical nature. Creating a list of politically binding measures has a better chance of success than creating 'hard law' obligations, as the process of treaty negotiations usually takes many years and bears the risk that technical developments overtake the treaty-drafting process.

Accordingly, the international community focuses current diplomatic endeavours on the development of CBMs for cyberspace as politically binding commitments.[104] This, however, does not diminish the practical value of CBMs. Declaratory statements of States are a powerful tool of international politics, and can define acceptable behaviour and de-escalation mechanisms in inter-State relations. Again, a glance at the existing arms control and disarmament regime shows that politically binding commitments present a practicable

[102] Goldsmith (n 13) 12.

[103] cf Günther Handl, 'Transboundary Impact' in Daniel Bodansky, Jutta Brunnée and Ellen Hey (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007) 531, 538ff; *Gabčikovo-Nagymaros Project* (1997) ICJ Rep 7, para 53; *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion (1996) ICJ Rep 226, para 29.

[104] See Hague (n 32).

and effective alternative to legally binding obligations as, for example, in the case of the *Hague Code of Conduct against Ballistic Missile Proliferation*[105] of 2002, or the two sets of guidelines[106] of the Nuclear Suppliers Group of 1978 and 1992 (subsequently amended).

3.4.2. Regional versus Global

Given the difficulties in agreeing a set of CBMs for cyberspace on the wider international level, the question arises as to whether such measures should rather be negotiated and endorsed at a regional level.

On the one hand, a regional approach could have a better chance of success, as multiple regional characteristics,[107] such as the level of modernity of critical infrastructure systems, specific political relations between neighbouring States, history and, finally, yet importantly, mentality could be considered in a more suitable manner. Additionally, a common understanding and notion of threat is also usually easier to achieve in regional agreements.[108] Finally, the development of regional CBMs would correspond with the tendency within the disarmament and arms control regime to conclude CBMs for regional and even localised crisis situations, as explicitly encouraged by the OSCE *Vienna Document* of 1999 and 2011 (para. 3.2.).[109] On the other hand, a global approach to CBMs for cyberspace is, if achievable, rather appropriate, as the internet is a global resource and cyber threats are thus challenges of a global nature. On a rather conceptual level, this finding is supported by the multitude of theories of interdependence in international relations and the sociology of globalisation.[110]

As mentioned above (para. 3.3.), apart from the nearly universal organisation UN and a few particular bilateral endeavours, two regional organisations, namely OSCE and ASEAN, are currently working on the development of CBMs for cyberspace. This, however, does not indicate a general tendency within the international community to develop CBMs for cyberspace at a regional level. The OSCE considers itself a regional (security) organisation (in the meaning of Chapter VIII of the UN Charter). However, the organisation can hardly be deemed regional in geographical terms, as it comprises 57 States from Europe, Central Asia and North America, reaching 'from Vancouver to Vladivostok'.[111] The ASEAN member States,

[105] The HCOC is the only multilateral transparency and confidence building instrument concerning the spread of ballistic missiles. Currently 134 States subscribed to the code, cf <http://www.hcoc.at>.

[106] *Guidelines for Nuclear Transfers* of 1978 and *Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software, and Related Technology* of 1992 (both subsequently amended).

[107] On different cyber profiles of States see Choucri (n 13) 92-124.

[108] cf UN Office for Disarmament Affairs (n 38).

[109] cf Lachowski (n 37) 11-14.

[110] For a discussion of 'regionalism' in international relations and international legal policy see International Law Commission (ILC), *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law* (Report of the Study Group of the International Law Commission, finalized by Martti Koskenniemi, UN Doc No A/CN.4/L.682, 13 April 2006) para 85.

[111] OSCE (n 56).

although, 'shar[ing] the view that regional CBMs should take into consideration the characteristics of the region',[112] decided in 2011 at an ASEAN Regional Forum (ARF) conference that, in future, ARF would work together with OSCE on developing CBMs for global cyber security.[113]

3.5. Obstacles and Challenges for CBMs for Cyberspace

Based solely on the specific characteristics of the internet, several obstacles and challenges for the effectiveness of such measures can be identified.

Most importantly, anonymity of action in cyberspace, identified above as rendering any legal obligation of States *de facto* futile (para. 3.4.1.), could at first sight also inhibit the effectiveness of political commitments. The possibility of conducting covert governmental cyber operations seems as potentially minimising the political risk of States to an extreme, and therefore increasing the risk of misperception and improper response to malicious cyber activities. Indeed, despite all political endeavours, and against the background of technological possibilities to act anonymously in the internet, States can retain a high degree of deniability with regard to their cyber activities. Additionally, activities and intentions of States with regard to their cyber capabilities are characterised by a high level of secrecy. From a rather sceptical point of view, as taken by one author,[114] this could result in the ineffectiveness of any transparency measures, e.g., the exchange of (actual) military concepts or of any other significant information. Thereby, the confidence aspect of CBMs, and thus the core aims and purposes of the respective commitments, would prove *de facto* to be in vain. However, this position does not distinguish between trust (or confidence) and assurance, the latter of which, according to sociological and philosophical studies, occurs in situations where risk of disappointment is low.[115] Online trust of a higher intensity occurs especially in situations where assurance is low, i.e., in less structured environments; a finding which provides a compelling argument against the idea that trust needs a constraining background of norms and commonly shared values to emerge.[116] Additionally, trust, as opposed to assurance, is a facilitator[117] in social interactions; an idea which can also be applied to inter-State relations. Thus, anonymity, which prevents effective deterrence as well as legal 'retaliation', and which is one of the reasons for negotiations of CBMs, can be deemed at the same time as the very reason for the establishment of trusting relationships between States. All in all, the trust (or confidence) can only be considered futile, if it is disappointed by certain behaviour.

---

[112] Kwon Haeryong, *The ARF Perspective on TCBMs: Future Work* (UNIDIR, Cyber Security Conference 2012: The Role of Confidence Building Measures in Assuring Cyber Stability, Geneva, 8–9 November 2012) slide 6 <http://www.unidir.ch/files/conferences/pdfs/pdf-conf1912.pdf>.

[113] Federal Republic of Germany (n 19).

[114] Lewis (n 15) 12 and 55.

[115] cf Matteo Turilli, Antonino Vaccaro and Mariarosaria Taddeo, 'The case of on-line trust' (2010) 23 Knowledge Technology and Policy Journal (3-4) 338ff.

[116] ibid 339.

[117] ibid 342.

Furthermore, the concept of CBMs for cyberspace does not embrace the notion that malicious cyber tools are foremost an asymmetric means of power. Malicious software is a powerful tool in the hands of 'super-empowered angry individuals' (freely adapted from Samuel Huntington's *The Clash of Civilisations*).[118] It will be difficult to prevent 'loss of control' and to de-escalate any stand towards other States in a situation of a cyber crisis (supposedly) caused by determined, and most probably anonymously acting non-State actors. Cyber tools are also the perfect means in the hands of politically unstable States, which are otherwise militarily inferior. These States are potential risk factors for international peace and security in the context of cyberspace, given that cyber tools are a relatively powerful and comparatively inexpensive means that can be obtained on demand. It could prove disadvantageous to disregard such potential within the context of negotiations of CBMs for cyberspace with regard to negotiation partners (e.g., focusing on 'like-minded' States).

Finally, despite the unique characteristics of the internet, the concept of CBMs for cyberspace has not yet approached the notion of considering the potential of de-escalation of certain non-State actors in a cyber crisis situation. CBMs aim to prevent the outbreak of an (international) armed conflict through 'loss of control' and inappropriate escalation of a cyber crisis situation, by establishing practical measures and processes of (preventive) cyber crisis management between States. This notion is rightly based on the reasoning that war or an international armed conflict can exist between States only. Consequently, negotiations of practical measures aiming to prevent a war or an (international) armed conflict would be a matter of inter-State relations, excluding any consideration of the de-escalation potential of non-State actors. However, this traditional notion does not fully appreciate the unique characteristics of the internet, the probabilities of cyber crisis scenarios and realities of the global cyberspace, which is shaped, driven and managed mainly by non-State actors. Data streams sent from computer systems located on a foreign State's territory, entering through technical components located on the State's own territory (being further transferred, e.g., to governmental, including military, networks) are managed by so-called tier 1 internet service providers (ISPs). In most developed democratic States, tier 1 ISPs are privately owned. These companies are the actors who would probably first notice damaging data streams of an intensity and quality relevant to national security, and undertake practical crisis management measures. Therefore, being the 'gate' for international interaction in data transmission, the role and practical de-escalation potential of tier 1 ISPs (e.g., technical information exchange with other States' tier 1 ISPs) could prove most valuable in the context of practical measures of international cyber crisis management. On the opposite end of the scale, an 'isolatory' approach at the international political level, disregarding the above-mentioned potential of non-State actors, could eventually render international cyber crisis management ineffective, and shift it *de facto* to the technical level, especially to global, informal cooperation fora, e.g., the Forum of Incident Response and Security Teams (FIRST).[119]

[118] cf Choucri (n 13) 226ff.

[119] FIRST is a global network of computer security incident response and security teams from government, commercial, and educational organisations that work together voluntarily to deal with computer security problems and their prevention, see further information at <http://www.first.org/>.

4. Relationship Between Political and Legal Commitments

As mentioned above (para. 3.4.1.), the international community is currently focusing its diplomatic endeavours on the development of CBMs for cyberspace of a politically binding nature. The value of political declarations should not be underestimated. In terms of practice, they can influence State behaviour in a powerful way. Apart from this, political commitments have some significance for international law.

There has always been a certain interdependency between policy and law. This is especially apparent in public international law, where States create norms by their behaviour in international relations, *inter alia,* by generally uniform and consistent practice accompanied by respective *opinio iuris*[120] (international customary law). The political discourse within the international community in the process of finding consensus for a joint political declaration can support the development of *opinio iuris* of the States. Therefore, negotiations preceding the formulation of political declarations, as well as the declarations *per se,* can support the development of future norms of customary international law.[121]

Furthermore, political declarations, especially when broadly supported within the international community, can support clarifying the content of international law norms of a rather general character, being thus a supportive means for the purposive interpretation of law.

In the context of CBMs for cyberspace, which are discussed at the international level as a substitute[122] for legally binding obligations, the concept of so-called 'soft law' becomes relevant. 'Soft law' comprises (apart from the category of resolutions of international organisations) non-binding agreements between States.[123] It can emerge when the international community identifies the need for regulation; however, reaching a comprehensive consensus resulting in the development of a legal norm (conventional or customary international law) seems not to be successful.[124] 'Soft law' is a practical means in international relations to fill such a gap. Being 'in the twilight between law and politics',[125] 'soft law' is described in scholarly writings as showing a certain proximity to law, and having the capacity to produce certain legal effects by shaping common expectations concerning

[120] *Opinio juris* refers to the belief of States that a certain State practice is permitted or required under international law. *Opinio juris* is an aspect necessary for the development of international customary law, cf Malcolm N. Shaw, *International Law* (6th edn, Cambridge University Press 2008) 84ff; Rüdiger Wolfrum, 'Sources of International Law' in MPEPIL (n 1) MN 25.

[121] cf Wolfrum (n 120) 63.

[122] See Hague (n 32).

[123] Categorisation according to Daniel Thürer, 'Soft Law' in MPEPIL (n 1) MN 10-17.

[124] Wolff Heintschel von Heinegg, 'Die weiteren Quellen des Völkerrechts' in Knut Ipsen (ed), *Völkerrecht* (6th edn, CH Beck, 2010) § 20 MN 21.

[125] Thürer (n 123) ch. I.

State conduct in international relations (in terms of the principles of good faith and estoppel[126]).[127] Furthermore, it has the benefit that rules which are not legally binding can first prove their value and practicability within international relations before becoming a 'hard law' obligation.[128] It should be mentioned that some scholars are sceptical of the 'soft law' concept because of the risk of blurring the line between law and political commitments.[129] Convincingly, it is asserted that 'soft law' is only of a speculative nature *ex ante*, and can be of value only *ex post*, explaining the evolution of a certain norms of international conventional or customary law.[130]

However, *ex ante* 'soft law' can be also useful as a means of a purposive interpretation of international law.[131] CBMs for cyberspace, being a political declaration or even 'soft law', will certainly support the interpretation of public international law as applicable to cyberspace, especially with regard to general principles of international law as described in the following sections.

5. Legal Implications: General Principles of International Law

As stated above, CBMs for cyberspace that were concluded bilaterally and are recommended or currently negotiated within the fora of international organisations are meant to have the nature of political commitments. These political commitments can support the interpretation of international law, as pertaining to international peace and security in cyberspace. It will be shown that such aspects are sparely regulated within the sources of international law listed in Article 38(1) of the *Statute of the International Court of Justice* (ICJ Statute). However, the aspects of international peace and security in cyberspace are also governed by general principles of international law. These principles are most important in the cyber context, since they form the basis for a progressive development of international law, enabling the international law system to respond to the dynamic needs of an international society and especially to meet the fast growing technological advances. An interpretation of the principles can be supported by the notion of what States consider as politically acceptable and feasible, as reflected in the sets of (draft) CBMs for cyberspace.

Article 38(1) of the ICJ Statute of 1945 identifies the sources of international law, which the Court shall apply, as including:

---

[126] Principle of non-contradiction of their own conduct (*non licet venire contra factum proprium* or *allegans contraria non audiendus est*); see Oscar Schachter, 'The Twilight Existence of Nonbinding International Agreements' (1977) 71 American Journal of International Law (2) 296. For references to international courts application of the principle of estoppel see Thomas Cottier and Jörg Paul Müller, 'Estoppel' in MPEPIL (n 1).

[127] Thürer (n 123) 9, 27-28.

[128] ibid.

[129] Heintschel von Heinegg (n 124) § 20 MN 22; Wolfrum (n 120) 63.

[130] ibid.

[131] cf Thürer (n 123) 29.

'a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;

b. international custom, as evidence of a general practice accepted as law;

c. the general principles of law recognized by civilized nations [...]'.

Although the provision is partly referred to as an authoritative[132] listing of sources of international law, it should be deemed as a declaratory statement of which sources existed when the provision was drafted.[133] It originates from Article 38 of the *Statute of the Permanent Court of International Justice* (PCIJ Statute) of 1920 and was reproduced in the ICJ Statute without considerable discussion and with only minor[134] alterations.[135] Nowadays, binding decisions of international organisations and unilateral acts of States are also acknowledged to have the potential of qualifying as sources of international law.[136] In the following, the legal implications for CBMs for cyberspace pursuant to the aforementioned sources of international law will be presented.

There are several international treaties which apply to State activities in cyberspace, including, for example, the UN Charter and the *Constitution* and *Convention of the International Telecommunication Union*. In contrast to a multitude of political mechanisms of cooperation in the arena of cyber security, only a few international treaties can be considered as mirroring the political commitments as adopted, recommended or currently negotiated within the framework of CBMs for cyberspace. These are predominantly international agreements pertaining to cooperation in (criminal) law enforcement (as mentioned by the UN GGE recommendations on CBMs for cyberspace, para. 3.3.1.). Examples are the *Convention on Cybercrime* of 2001 (Chapter III), and the agreements establishing INTERPOL and its 'cybercrime programme'[137] as well as the EU's law enforcement agency EUROPOL and its newly established *European Cybercrime Centre.*[138] Additionally, Article VI of the bilateral *Agreement on the Prevention of Dangerous Military Activities*[139] (concluded between the US and USSR in 1989 and between Canada and USSR in

[132] cf Wolfgang Friedmann, 'The Uses of "General Principles" in the Development of International Law' (1963) 57 American Journal of International Law 279; James Crawford, *Brownlie's Principles of Public International Law* (8th edn, Oxford University Press 2012) 22 (with further references).

[133] Wolfrum (n 120) 10. For a criticism on formulation and completeness: JP Tammes, 'The Legal System as a Source of International Law' (1953) 1 Netherlands ILR (4) 374.

[134] Alterations were made in the numbering of the paragraphs and subparagraphs (instead of alphabetic characters) and the addition of a few words in the introductory phrase.

[135] Alain Pellet, 'Art. 38' in Andreas Zimmermann et al. (eds), *The Statute of the International Court of Justice. A Commentary* (Oxford University Press 2006) MN 42-45; Giorgio Gaja, 'General Principles of Law' in MPEPIL (n 1) MN 4.

[136] Heintschel von Heinegg (n 124) § 16 MN 17, 23; Wolfrum (n 120) 10; Pellet (n 135) 96, 88-95 (with further references to ICJ jurisprudence and State practice).

[137] Interpol <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>.

[138] EUROPOL <https://www.europol.europa.eu/ec3>.

[139] See supra n 90.

1991, and still in force with the successor to the USSR, the Russian Federation) resembles the characteristics of a CBM applicable to cyberspace; it states that any 'interference' with military 'command and control networks' (which could cause harm to personnel or damage to equipment) is regarded as a dangerous military activity, which (according to Article VII) results in certain de-escalation procedures by the armed forces of the Parties, including notification via pre-established communication lines, information exchange, and termination of interference. However, the provision is applicable to activities 'in proximity to personnel and equipment of the armed forces of the other Party', and thus will only seldom apply to activities conducted via the internet (which can be easily carried out from greater distance).

Another source of international law, as stated in Article 38(1)(b) of the ICJ Statute, is 'international custom, as evidence of a general practice accepted as law'. Despite some criticism[140] as to the logic of the phrasing, it is generally accepted in scholarly writings[141] and confirmed by the jurisprudence of the ICJ[142] that the identification of a customary rule requires two elements: (1) a generally uniform and consistent State practice (according to some scholars, no particular duration of the practice is required) and (2) the *opinio iuris sive necessitatis*, i.e., the belief that the behaviour is required or permitted under international law. Other than in the realm of international cooperation in law enforcement, very little reliable information is available on actual State practice in cyberspace, as it is relevant to international peace and security. This is due to the clandestine nature of cyber intelligence operations and to the secrecy that surrounds offensive military cyber operations, which might have taken place in the past. *Opinio iuris* is equally difficult to identify, even separately from any State practice (that is currently publicly not detectable), due to lack of official governmental statements by States on the legality or illegality of (potential) governmental cyber activities relevant to international relations. This does not mean that the existing norms of customary international law, e.g., the prohibition of the use of force in international relations (enshrined in Article 2(4) of the UN Charter), would not apply to governmental cyber activities, following a respective interpretation of the norm in question. However, *cyber-specific* norms of international custom, in particular those reflecting the contents of the previously presented sets of CBMs, are currently not detectable.

'[G]eneral principles of law recognized by civilized nations' within the meaning of Article 38(1)(c) of the ICJ Statute are a (subsidiary)[143] source of international law which is derived, according to the wording and as understood by the majority of scholars, from principles common to the domestic law systems of all 'civilised'[144] countries, in so far as they are

[140] It is rather the general practice accepted as law which provides the evidence for the existence of custom. cf Pellet (n 135) 207, Wolfrum (n 120) 24.

[141] eg Wolfrum (n 120) 25; Tullio Treves, 'Customary International Law' in MPEPIL (n 1) MN 17ff (with references to ICJ jurisprudence); Pellet (n 135) 201; cf Crawford (n 132) 23-30 (detailed discussion of the elements of customary international law).

[142] eg *North Sea Continental Shelf,* Judgement (1969) ICJ Rep 3, para 77.

[143] Pellet (n 135) 290; contra: Gaja (n 135) 21.

[144] The reference to 'civilised' nations was included in Article 38 of the *Statute of the Permanent Court of Justice* (League of Nations) of 13 December 1920 (and was reproduced in the *Statute of the International Court of Justice*). During these times of euro-centric international law understanding, it was meant to exclude the rather 'primitive' law systems; nowadays, it does not have any discriminatory meaning, cf Heintschel von Heinegg (n

applicable to inter-State relations.[145] The general principles are identified by a method of successive inductive 'accretions' based on a comparison of the principal systems of law.[146] Such principles are, e.g., responsibility and reparation for damages, unjust enrichment, property and indemnity.[147] Additionally, general principles of law contain a multitude of rules of procedural nature, as confirmed by the PCIJ and ICJ in a number of cases.[148] Due to the fact that matters of relevance to international peace and security are to be located at the level of international relations and not in municipal law, *cyber-specific* rules of general principles derived from national law systems cannot be identified within that source of international law.

Furthermore, decisions of international organisations show the potential to be recognised as a source of international law, as they can evidence a certain *opinio iuris* of their member States.[149] Partly, also 'recommendations' of international organisations, such as resolutions of UNGA (see Article 13(1) of the UN Charter) are acknowledged to have some 'normative value' in terms of the emergence of *opinio iuris* (as stated by the ICJ in the *Nuclear Weapons*[150] advisory opinion) or as part of 'soft law'.[151] However, the UNGA resolutions referring to the *Developments in the field of information and telecommunications in the context of international security*[152] or to the *Creation of a global culture of cybersecurity*[153]

---

124) § 17 MN 2. However, Bassiouni claims that the expression still has utility when a given nation, because of peculiar historical circumstances, no longer follows its previously 'civilised' system of law, or that of the other 'civilised nations'. cf Mahamoud Cherif Bassiouni, 'A Functional Approach to General Principles of International Law' (1990) 11 Michigan Journal of International Law 768.

[145] Heintschel von Heinegg (n 124) § 17 MN 1; Brian D. Lepard, *Customary International Law. An New Theory with Practical Implications* (Cambridge University Press 2010) 164; Crawford (n 132) 34ff (with further references on the different opinions). For a discussion of the methodology see Stephen C. Hicks, 'International Order and Article 38(1)(c) of the statute of the International Court of Justice' (1978) 2 Suffolk Transnational Law Journal (1) 1-42. Petersen considers also 'general principles of international law' as covered by the norm (by analogy), see Niels Petersen, 'Customary Law Without Custom? Rules, Principles, and the Role of State Practice in International Norm Creation' (2008) 23 American University International Law Review 308.

[146] Similarly Robert Kolb, 'Principles as Sources of International Law (With Special Reference to Good Faith)' (2006) 53 Netherlands International Law Review (1) 10; Pellet (n 135) 258; Friedmann (n 132) 282; Crawford (n 132) 35 (stating that tribunals have adopted modes of general reasoning as well as comparative law analogies). For a discussion of the methodology see Hicks (n 145); Bassiouni (n 144) 788-792 (with examples of ICJ jurisprudence).

[147] Heintschel von Heinegg (n 124) § 17 MN 4; other proposals at Friedmann (n 132) 287.

[148] eg *Article 3, Paragraph 2, of Treaty of Lausanne,* Advisory Opinion (1925) PCIJ Rep Ser B, No 12, 32 (referring to the 'well-known rule that no one can be judge in his own suit'); *The Corfu Channel Case,* Merits, (1949) ICJ Rep 4, 18 (allowing the use of indirect proof of culpability of a State concerning events occurring within its frontiers and pointing out that such 'indirect evidence is admitted in all systems of law, and its use is recognized by international decisions'); *Nuclear Tests (Australia v. France)* (1974) ICJ Rep 253, para 46 (affirming that a basic principle of legal obligation 'is the principle of good faith'); *Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights,* Advisory Opinion (1999) ICJ Rep 62, para 63 (asserting that there 'is a generally recognized principle of procedural law' that 'questions of immunity are [...] preliminary issues which must be expeditiously decided *in limine litis*'); see also overview at Gaja (n 135) 8-16.

[149] See supra n 136.

[150] Nuclear Weapons (n 103) 70.

[151] Heintschel von Heinegg (n 124) § 16 MN 23; Pellet (n 135) MN 105.

[152] See supra n 60.

[153] See supra n 61.

do not seem to have the authoritative character which could lead to the assumption that their content, in whole or part, developed a 'normative value'. This assessment is justified by the fact that neither States nor academia (whose opinions are a subsidiary means for the determination of rules of law pursuant to Article 38(1)(d) of the ICJ Statute) refer to these resolutions by claiming their (*quasi*) authoritative or persuasive nature. The author of the present paper is equally not tempted to do so, as the resolutions rather appear as automatically repeated acknowledgments of cyber threats as pertaining to international peace and security.

Similarly, specific unilateral *acts* (including, e.g., proclamations)[154] of States invoking legal (in contrast to political) obligations, which could be deemed to mirror the content of the sets of CBMs previously presented or referring to international peace and security in the cyber context, are not perceivable. Especially, national cyber security strategies[155] which, in general terms, address the need for international cooperation in encountering cyber threats, cannot be considered as invoking legal obligations.

The above assessment does not mean that cyberspace and its aspects relevant to international peace and security is to be considered a legal *lacuna*.[156] The classical international law approach to a situation which is not or only partly regulated by law, would be to invoke the basic principle as stated by the PCIJ in the *Lotus*[157] case: based on the notion of sovereignty, in the absence of a legal prohibition, a State enjoys freedom of action. However, the consequently competing freedoms of the coexisting sovereign States are guided (and de-conflicted) by general principles of international law. Thus, although being regulated by contractual norms with regard to singular aspects only and lacking *specific* regulations of customary law, general principles deriving from municipal laws, binding decisions (or recommendations) of international organisations or unilateral acts of States invoking legal obligations, cyberspace is governed by the existing general principles of international law.

In the following, the nature of general principles of international law will be described (5.1.), followed by an examination of several specific principles and their application to cyberspace, focusing on aspects as addressed in the respective sets of (draft) CBMs for cyberspace (5.2.). Finally, some thoughts on *lex ferenda* for cyberspace, in terms of an application of general principles of international law deducted from legal regimes governing shared resources or common spaces, will be presented (5.3.).

---

[154] Heintschel von Heinegg (n 124) § 16 MN 17.

[155] See supra n 3.

[156] Unfortunately, some authors (US Air Force) deduct from the fact that States do not publicly comment on certain malicious cyber activities as reported by the media and committed by unknown actors that all cyber activities below the threshold of use of force are permitted in terms of international custom, see Gary Brown and Keira Poellet, 'The Customary International Law of Cyberspace' (2012) 6 Strategic Studies Quarterly 126-145. Such a position disregards the fact that customary rules other than prohibition of the use of force (and those general principles of international law which do have the nature of customary law at the same time) do apply to governmental cyber operations in the way of interpretation of law.

[157] cf *The Case of the S.S. 'Lotus',* Merits (1927) PCIJ Rep Ser A, No 7, 18ff.

5.1. Nature

The term 'principles' may refer to a meta-legal concept, generated within a philosophical or ethical discourse, or to principles inherent in or developed from a particular body of law or law in general.[158] General principles of international law belong to the latter category, and must be distinguished from the notion of 'justice' (or equity in the broad sense) and from 'general principles of moral law', i.e., compelling or essential ethical principles endorsed in international law (e.g., prohibition of genocide).[159] On a conceptual level, though, the ethical and legal meaning of the term 'principles' cannot be completely separated, as legal principles are always to be deemed as expressions of overarching values.[160] General principles of international law reflect a genuine morality and the most basic values of the international society, as inherent in the international order and absolute principles relative to that existing order.[161] It should be mentioned that, because of this feature, general principles of international law are partly criticised in academic writings as being a 'gateway into the legal discourse for natural law maxims'.[162]

As stated by one scholar, 'general principles of law [...] [are] arguably the most important but certainly the least used and most confused source of law [...]'.[163] The jurisprudence of the ICJ does not bring clarity to the matter, as hitherto the Court's reference to general principles of international law has been 'inconsistent and confused'.[164] The academic controversy pertains in particular as to whether general principles of international law can be deemed as a source of law of a normative character or merely reflecting juridical maxims or legal ideas. In addition, there are disagreements over whether they can present a source of obligations for States, whether they are a source of natural law, and which relation they show with regard to that concept; whether they are enshrined in Article 38(1)(c) of the ICJ Statute, or are part of customary international law within the meaning of Article 38(1)(b) of the ICJ Statute, even of a peremptory character, or whether they exist aside from the enumeration of the aforementioned Article as an autonomous source of law; and whether they have a merely persuasive authority of interpretative guidance or have the a nature of a *quasi*-constitutional norm of most important character.

---

[158] Rüdiger Wolfrum, 'General International Law (Principles, Rules, and Standards)' in MPEPIL (n 1) MN 6; idem (n 120) MN 33.

[159] Lepard (n 145) 165; Bassiouni (n 144) 775. The ICJ has made a distinction between legal rules and 'moral principles' which can be taken into account 'only in so far as these are given a sufficient expression in legal form', see *South West Africa,* Second Phase (1966) ICJ Rep 5, para 49.

[160] Armin von Bogdandy, 'General Principles of International Public Authority: Sketching a Research Field' (2008) 9 German Law Journal 1912; Bassiouni (n 144) 775.

[161] Lepard (n 145) 164; Hicks (n 145) 24ff, 27; Bassiouni (n 144) 784ff (with further references).

[162] Petersen (n 145) 292 (with further references).

[163] Hicks (n 145) 7. For reasons of correctness, it should be noted, that Hicks refers specifically to '*general principles of law recognized by civilized nations* [pursuant to] Article 38(1) (c) of the Statute of the International Court of Justice', however, the context allows us to conclude that he interprets the norm as including also the notion of general principles of international law.

[164] ibid 34.

Thus, it is surely not an exaggeration to assert that every aspect of general principles of international law is disputed and unclear. Against this background, a thorough presentation of diverse scholarly opinions on the specific aspects of controversy, as well as a clarification with regard to the respective legal debate must be considered a task for a legal analysis of a major extent and cannot be provided for within the limited scope of the present paper. Therefore, the following assessment can only offer a limited overview of the relevant court rulings and opinions of legal commentators, and attempt to describe the source and content (5.1.1.), and the categorisation (5.1.2.) of general principles of law, the distinctive status they enjoy within the international law system (5.1.3.), and their feature as a vehicle of progressive law development (5.1.4.).

5.1.1. Source and Content

'[G]eneral principles of law recognized by civilized nations' pursuant to Article 38(1)(c) of the ICJ Statute are mostly understood in the sense that they are sources of international law, but derive from municipal law systems.[165] Some scholars assert that the provision also includes general principles of international law, reflecting rather the international order of States than the national law systems.[166] They refer to the PCIJ Statute's *travaux préparatoire* of 1920, which shows that the drafters had different views of the reference to 'general principles of law', including the notion that the principles are to be understood in a broad way as 'maxims of law'.[167] Furthermore, the drafting history shows that Article 38(c) (or as it was then, No. 3) was a response to the need for the completeness[168] of the law and the intention of the drafters was to avoid a *non liquet* of the Court for lack of a positive rule (however, without giving the judges the possibility to legislate or opening a gateway for natural law).[169] In this spirit, it is asserted that a modern interpretation of Article 38 is justified by the changes of the structure of the legal order since 1920 with regard to the means of determination of international rules based on an implicit consensus of the States, which nowadays can be derived from more than the municipal legal systems, but also, e.g., from binding decisions of international organisations.[170] Finally, it is noted that general

[165] Pellet (n 135) MN 251.

[166] eg Hicks (n 145) 42; Bassiouni (n 144) 772; Petersen (n 145) 307ff; Wolfrum (n 158) 28 (with further references); Crawford (n 132) 37 (asserting that general principles of international law refer to Article 38(1)(c) of the ICJ Statute, as well as to customary law or to certain logical propositions underlying judicial reasoning).

[167] On drafting history see Gaja (n 135) 3; Pellet (n 135) 17-41; Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals* (Cambridge University Press 1953) 6-21.

[168] In 1920, customary law was considered a slowly developing source of international law. Additionally, the development of new rules of customary law was these days surrounded by a scepticism, given the newly appeared heterogeneity of the international community by the establishment of the Marxist-Leninist regime of USSR. Moreover, international treaty law was not as extensive as it is today, as the majority of the treaties (currently over 50,000 are registered at the UN) were concluded after 1945. See Kolb (n 146) 30 (with further references).

[169] cf Bassiouni (n 144) 772ff, 779; Petersen (n 145) 307ff; Pellet (n 135) 245 (with further references to the drafting history); Kolb (n 146) 30.

[170] Petersen (n 145) 308.

principles as mentioned in the ICJ Statute and general principles of international law cannot always be distinguished from each other.[171]

Others[172] assert that the reference to recognition by nations constitutes the distinguishing element between the principles referred to by Article 38(1)(c) of the ICJ Statute and the general principles of international law, of which only the latter derive from international law. Advocates of this approach also invoke the legislative history, object and purpose of Article 38(1)(c) of the ICJ Statute as a supporting argument.[173] Their view is supported by the wording of Article 21(1) of the *Rome Statute of the International Criminal Court* of 1998, which describes as the law applicable by the Court, *inter alia*, 'principles and rules of international law' (lit. b) and 'general principles of law derived by the court from national laws of legal systems of the world' (lit. c), thus explicitly distinguishing between the two forms of 'general principles'. As the *Rome Statute* hitherto has been signed by 139[174] States, it can be asserted that the majority of States, who are the primary subjects of international law, consider general principles of international law as existing aside from the general principles derived from national law systems, and consequently beside the enumeration of law sources in Article 38 of the ICJ Statute.

This view is confirmed by the jurisprudence of the PCIJ and ICJ, which indicates the existence of general principles of law, irrespective of their correspondence to principles pertaining to municipal laws.[175] The PCIJ, for example, referred to 'principles of international law',[176] 'an elementary principle of international law',[177] 'a principle of international law, and even a general conception of law',[178] 'general and essential principles',[179] 'generally accepted principle of international law',[180] and to a 'principle universally accepted'.[181] The ICJ, e.g.,

[171] Wolfrum (n 158) 20; Bassiouni (n 144) 774.

[172] eg Pellet (n 135) 86 and 252; Tammes (n 133) 374; Wolfrum (n 158) 7 and 20; cf Heintschel von Heinegg (n 124) § 17 MN 1; Hicks (n 145) 3ff, 7, 35; Lepard (n 145) 163 and 166; Gaia (n 135) 32.

[173] Wolfum (n 158) 28.

[174] Information of the UN Treaty Collection as of 9 May 2013, <http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10&chapter=18&lang=en>.

[175] cf Gaia (n 135) 32.

[176] Lotus (n 157) 31.

[177] *Mavrommatis Palestine Concessions,* Judgement (1924) PCIJ Rep Ser A, No 2, 12 (referring to the principle that a State has a right to protect its subjects when injured by unlawful acts committed by another State).

[178] *Case Concerning the Factory at Chorzów,* Merits (1928) PCIJ Rep Ser A, No 17, 29 ('any breach of an engagement involves an obligation to make reparation').

[179] ibid 47-48.

[180] *Greco-Bulgarian 'Communities',* Advisory Opinion (1930) PCIJ Rep Ser B, No 17, 32 ('in relations between treaty parties treaty law prevails over municipal law').

[181] *Electricity Company of Sofia and Bulgaria,* Order (1939) PCIJ Rep Ser A/B, No 79, 199 ('[…] parties to a case must abstain from any measure capable of exercising a prejudicial effect with regard to the execution of the decision to be given, and, in general, not allow any step of any kind to be taken which might aggravate or extend the dispute').

invoked 'general and well recognized principles',[182] 'rule[s] of law generally accepted',[183] 'general principles of international law',[184] 'fundamental or cardinal principle of [...] law',[185] 'fundamental principle of international law',[186] 'well established principle of international law',[187] and a 'principle universally accepted'.[188] In none of the cases, was the Article of the 38(1)(c) ICJ Statute mentioned in the context.

The question arises, upon which methodology the existence of general principles of international law is recognised. The assertion by the ICJ of a general principle of law was only rarely accompanied by an adequate demonstration of its existence in international law.[189] In the *Lotus* case, the PCIJ conducted 'researches [of] all precedents, teachings and facts to which it had access and which might possibly have revealed the existence of one of the principles of international law […]'.[190] In the *Chorzów Factory* case, the Court ascertained an 'essential principle', because it 'has […] never been disputed in the course of the proceedings in the various cases concerning the Chorzów factory'[191] and 'seem[ed] to be established by international practice and in particular by the decisions of arbitral tribunals'.[192] In the *Electricity Company of Sofia and Bulgaria* case, the PCIJ concluded the existence of a principle, because it was 'universally accepted by international tribunals and likewise laid down in many conventions',[193] without further explanation. The ICJ sought in the *Nicaragua*

[182] Corfu Channel (n 148) 22 ('[...] certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war; the principle of the freedom of maritime communications; and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'); Nicaragua (n 96) 215 ('certain general and well recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war').

[183] *Right of Passage over Indian Territory Case,* Preliminary Objections, (1957) ICJ Rep 125, 142 ('Once the Court has been validly seized of a dispute, unilateral action by the respondent State in terminating its Declaration, in whole or in part, cannot divest the Court from its jurisdiction').

[184] *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970),* Advisory Opinion (1971) ICJ Rep 16, para 94 ('the general principles of international law regulating termination of a treaty relationship on account of breach').

[185] Nicaragua (n 96) 190 ('A further confirmation of the validity as customary international law of the principle of the prohibition of the use of force expressed in Article 2, paragraph 4, of the Charter of the United Nations may be found in the fact that it is frequently referred to in statements by State representatives as being not only a principle of customary international law but also a fundamental or cardinal principle of such law.'); ibid 181 ('common fundamental principle').

[186] *Applicability of the Obligation to Arbitrate under Section 21 of the United Nations Headquarters Agreement of 26 June 1947,* Advisory Opinion (1988) ICJ Rep 12, para 57 ('the fundamental principle of international law that international law prevails over domestic law').

[187] *Case Concerning Land and Maritime Boundary Between Cameroon and Nigeria Case (Preliminary Objections),* Judgement (1998) ICJ Rep 275, para 38 ('the principle of good faith is a well-established principle of international law').

[188] *LaGrand Case,* Judgement, (2001) lCJ Rep 466, para 103.

[189] Gaia (n 135) 20.

[190] Lotus (n 157) 31.

[191] Chorzów Factory (n 178) 29.

[192] ibid 47.

[193] Electricity Company of Sofia and Bulgaria (n 181) 199 ('[…] parties to a case must abstain from any measure capable of exercising a prejudicial effect in regard to the execution of the decision to be given, and, in general, not allow any step of any kind to be taken which might aggravate or extend the dispute').

case, 'confirmation of the validity as customary international law of the principle of the prohibition of the use of force' by reference to Article 2(4) of the UN Charter and 'the fact that it is frequently referred to in statements by State representatives as being not only a principle of customary international law but also a fundamental or cardinal principle of such law'.[194] In the *Western Sahara*[195] advisory opinion, the Court referred as the basis for the principle of international law of self-determination of peoples to the UN Charter, UNGA resolutions and to its own prior decision. Thus, it can be concluded that the jurisprudence of the international courts did not develop any methods of identifying general principles of international law. Unfortunately, to quote a scholar, '[s]cholarly writings on this question are few, and what writings exist are unclear.'[196] The most accurate assertion might be the ambiguous proposal to identify general principles of international law 'by way of successive "accretions" (inductive) and "concretization" (deductive) to which the principle leans itself'.[197]

By whichever methodology, academic literature and the jurisprudence of the PCIJ and ICJ indicates that general principles of international law can be derived from general considerations[198] (e.g., 'elementary considerations of humanity', see *Corfu Channel Case*[199]), legal logic (mostly pertaining to procedural rules), legal relations in general (e.g., principle of good faith),[200] from international relations, or from a particular treaty[201] regime (see advisory opinion on *Genocide Convention*[202]).[203] Additionally, some scholars assert that general principles of international law can be derived from the 'conception of [a specific] legal system'[204] (e.g., the UN) and may emerge from 'manifestations of international consensus expressed in [UN] General Assembly and Security Council Resolutions'.[205]

PCIJ and ICJ identified several principles of either general significance (freedom of maritime communications,[206] damages[207]), of a contractual nature (*pacta sunt servanda,*[208] good

[194] Nicaragua (n 96) 190.

[195] *Western Sahara,* Advisory Opinion (1975) ICJ Rep 12, para 54-65.

[196] Bassiouni (n 144) 817.

[197] cf Kolb (n 146) 10.

[198] Wolfrum (n 120) 37.

[199] Corfu Channel (n 148) 22.

[200] Wolfrum (n 120) 37.

[201] ibid (with examples).

[202] *Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide,* Advisory Opinion (1951) ICJ Rep 15, 23 ('the principles underlying the Convention are principles which are recognized by civilized nations as binding on States, even without any conventional obligation'); confirmed in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide,* Judgement (2007) ICJ Rep 43, 161.

[203] cf Hermann Mosler, 'General Principles of Law' in Rudolf Bernhardt (ed), *Encyclopedia of Public International Law* (vol 2, Elsevier North Holland 1995) 511-27; Wolfrum (n 158) 29; idem (n 120) 35.

[204] Tammes (n 133) 377ff (referring to the case *Effects of Awards of Compensation made by the United Nations Administrative Tribunal,* Advisory Opinion (1954) ICJ Rep 54).

[205] Bassiouni (n 144) 769.

[206] Corfu Channel (n 148) 22.

faith,[209] estoppel[210]), of procedural character (*nemo in re sua judex*)[211] and of relevance to specific situations (self-determination of peoples,[212] *uti possidetis juris*,[213] 'fundamental general principles of humanitarian law',[214] 'elementary considerations of humanity'[215]). Academic writings assert, beside the above-mentioned principles, the existence of further general principles of international law, such as consent, reciprocity, unjust enrichment, finality of settlements, and proportionality.[216] Additionally, based on the notion of general principles as systematisation of existing norms of international law, the 'principle of common heritage of mankind' (developed in the context of the law of the sea and applied to certain common spaces) and the 'principle of sustainable development' (developed in the context of international environmental law) is affirmed.[217]

With regard to general principles of international law *as pertaining to international peace and security*, the international courts did explicitly acknowledge the principles of State sovereignty[218] (and the corresponding principle of 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'[219]), non-intervention,[220] refraining from use of force in international relations,[221] and peaceful settlement of disputes.[222] Article 2 of the UN Charter enshrines these principles as legal obligations,[223] i.e., the sovereign equality of States (No. 1), non-intervention in matters within the domestic jurisdiction of States (No. 7, although only stating a respective prohibition for the UN), refraining from (threat or) use of force in international relations (No. 4), and peaceful settlement of disputes (No. 3). Article 1 of the UN Charter, depicting the purposes of the organisation, refers to the organisation's goal of achieving international

---

[207] Chorzów Factory (n 178) 29.

[208] Treaty of Lausanne (n 148) 12.

[209] Nuclear Tests (n 148) 46.

[210] *Case Concerning the Temple of Preah Vihear,* Merits (1962) ICJ Rep 6, 31-32.

[211] *South-West Africa Voting Procedure,* Advisory Opinion (1955) ICJ 67, 99-100.

[212] Western Sahara (n 195) 54-65; Namibia (n 184) 31 ('[..] the subsequent development of international law with regard to non-self-governing territories, as enshrined in the Charter of the United Nations, made the principle of self-determination applicable to all of them').

[213] *Case Concerning the Frontier Dispute,* Judgement (1986) ICJ Rep 554, para 20.

[214] Nicaragua (n 96) 218, 220, 225.

[215] Corfu Channel (n 148) 22.

[216] cf Brownlie (n 91) 19; Crawford (n 132) 37; Kolb (n 146) 25ff. As stated before, it is noted in the academic writings that some of the principles may not be distinguishable from the 'general principles of law recognized by civilized nations' in the meaning of Article 38(1)(c) of the ICJ Statute.

[217] Wolfrum (n 158) 8.

[218] Nicaragua (n 96) 263.

[219] Corfu Channel (n 148) 22.

[220] Nicaragua (n 96) 202, 204.

[221] ibid 181.

[222] ibid 290.

[223] Andreas Paulus, 'Article 2' in Bruno Simma et al. (ed), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012) MN 8.

cooperation in solving international problems (No. 3). All the above-mentioned principles of the UN and, additionally, the duty of States to cooperate are further elaborated upon in the UNGA *Friendly Relations Declaration*[224] of 1970 (widely accepted as a *quasi*-binding interpretation of the UN Charter),[225] which declares them to 'constitute basic principles of international law' (General Part, para. 3). These 'basic principles' were confirmed by the UNGA in its *Millennium Declaration*[226] of 2000. At the regional level, States participating in the *Conference on Security and Cooperation in Europe* in 1975 adopted a *Declaration on Principles Guiding Relations between Participating States*[227] (part of the so-called *Helsinki Declaration*), which affirms, apart from other principles, all the general principles of international law pertaining to international peace and security as stated in the *Friendly Relations Declaration*. Scholarly writings in general confirm these principles as having the nature of general principles of international law, partly adding also into this category the principle of domestic jurisdiction (correlating with State sovereignty).[228]

Thus, a common core of general principles of international law, as pertaining to international peace and security, can be identified, even if the finding is '[…] based on nothing grander than their having passed what Thomas Franck calls the 'but of course test' – a more or less unstable 'common sense of the international community' […]'.[229] In summary, general principles of international law as relevant to international peace and security can be deemed as consisting of the principles of:

- sovereign equality of States, including the correlated principles of:
    - self-preservation,
    - independence,
    - jurisdiction over domestic matters,
    - non-intervention in matters within the domestic jurisdiction of other States,
    - duty not to harm the rights of other States,
- maintenance of international peace and security, including the principles of:

[224] *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations* UNGA Res 2625 (XXV) (24 October 1970) annex (adopted without vote).

[225] Bardo Fassbender, 'Article 2(1)' in Simma (n 223) MN 31 (referring to the 'careful preparation and adoption by consensus', due to which the declaration 'can be relied upon almost like a text enjoying bonding force'). See also Paulus (n 223) 5; Helen Keller, 'Friendly Relations Declaration (1970)' in MPEPIL (n 1) MN 1 (referring to 'codification and progressive development of international law') and MN 31ff (showing the continuous reference to the resolution by UNGA, UNSC, ICJ, etc., with further references).

[226] *United Nations Millennium Declaration* UNGA Res 55/2 (8 September 2000) para 4.

[227] See supra n 39.

[228] cf Brownlie (n 91) 19; Crawford (n 132) 37 (naming the principles of equality of States and domestic jurisdiction); Kolb (n 146) 25ff (naming the principles of 'non-use of force, peaceful settlement of disputes […], etc.'); Heintschel von Heinegg (n 124) § 16 MN 43 (naming only the principle of equality and independence of States).

[229] ILC (n 110) 468 (with further references).

- restrain of (threat or) use of force in international relations,
- duty to peaceful settlement of disputes, and

- duty to international cooperation in solving international problems.

The significance and concretisation of these principles for cyberspace will be introduced in detail *infra*.

5.1.2. Normativity and Categorisation

Some scholars assert that, because of their generality, not all general principles of international law could have a binding authority in the meaning of normative requirements on States, but rather a persuasive authority in the meaning of guidelines.[230] Others, also addressing the general character of the principles, concur with this finding, referring to general principles as mere 'legal ideas'.[231] General principles of international law certainly do not show the level of specification of rules, which are formulated for practical purposes.[232] However, they are also distinct from abstractly formulated legal standards (e.g., 'due regard' or 'reasonable time'). Those 'concepts of law', mostly incorporated in legal norms, do not present a source of law, but support the subsuming of the facts of the case to the norm.[233] In contrast, general principles of international law show a core legal meaning developed over centuries, and thus present neither 'legal ideas' nor mere structural or guiding principles.[234]

However, during the 1960s, it was claimed that general principles of international law could not be deemed a source of law, because the legal principles governing the Western system, the system based on Marxism-Leninism, and the Islamic law system (preconditioned by compatibility with various interpretations of Islam) were very different.[235] In a more general manner, referring to the value-oriented nature of the principles, it was also asserted that a general consensus on values cannot be identified between the members of the international society.[236] Indeed, general principles of international law are characterised by serving the purpose of protecting a common or individual good, and are value-related.[237] However, this cannot be taken as an argument against the normative nature of general principles of international law, as it is true for the whole international law system. According to a broad group of scholars, (basic) universally shared values lay the foundation of international law,

[230] cf Lepard (n 145) 167.

[231] Kolb (n 146) 9.

[232] Wolfrum (n 158) 6; Cheng (n 167) 24; Kolb (n 146) 9.

[233] Kolb (n 146) 16ff, stating that, however, some legal standards as 'equity', 'goodwill' or 'good faith' proved to have been applied autonomously in arbitration of commercial law cases.

[234] cf von Bogdandy (n 160) 1912; Kolb (n 146) 8ff.

[235] Bassiouni (n 144) 782ff (with further references).

[236] Hicks (n 145) 6; Ingo Venzke and Jochen von Bernstorff, 'Ethos, Ethics, and Morality in International Relations' in MPEPIL (n 1) MN 3, 28.

[237] Petersen (n 145) 288.

aiming at safeguarding and promoting universal values and global goals.[238] Irrespective of the dichotomy of positivism *versus* naturalism, it is acknowledged today that any legal argument has constant recourse to extra-positive elements, which flow into the law by way of 'certain strong arguments or *topoi*, concentrated into a series of value-oriented general principles [...]'.[239] The concerns referring to ideological, religious and other value-based differences within the international society can be contested with a reference to the universal acceptance of the international law system's existence. General principles of international law are inherent to the system (and their general and basic nature allows different interpretations in concrete situations). Nevertheless, it will indeed be always important to delimit them from the extra-positive social or ethical principles,[240] or from the aforementioned 'general principles of moral law'.

All in all, general principles of international law are nowadays accepted by a vast majority of scholars as a normative source of law.[241] This finding is confirmed by the wording of the above-mentioned Article 21(1)(b) of the *Rome Statute* (declaring 'principles and rules of international law' as a source of law applicable by the International Criminal Court) as well as by the jurisprudence of the PCIJ and ICJ which relied upon general principles of law not only for interpretative purposes, but also to fill a gap in a situation which was not governed by contractual or customary law.[242]

However, controversy prevails with regard to the categorisation of general principles of international law within the sources of law. Some[243] scholars deem general principles of international law as being part of international customary law, even presenting peremptory norms (*ius cogens*) of international custom.[244] Others[245] recognise the principles as a separate source of international law, giving an impulse and directing the formulation of customary international law, however, being most difficult to distinguish from it. The jurisprudence of the ICJ does not support the drawing of a definite conclusion: the Court referred in the so-called *Hostages*[246] case to a principle of international law as being also a norm of customary law. In the *Nicaragua*[247] case, the Court stated that certain customary international law 'flow[s] from a […] fundamental principle'. Then, in the *Nicaragua*[248] case

[238] Venzke and von Bernstorff (n 236) 28.

[239] Kolb (n 146) 4.

[240] ibid.

[241] ibid; Heintschel von Heinegg (n 124) § 16 MN 43; Hicks (n 145) 11; Cheng (n 167) 23; Petersen (n 145) 277 and 287 (implicitly); von Bogdandy (n 160) 1912.

[242] See examples of the jurisprudence at Bassiouni (n 144) 798 (with further references).

[243] Heintschel von Heinegg (n 124) §16 MN 43; Treves (n 141) 1 and 19-22; Gaja (n 135) 24.

[244] Bassiouni (n 144) 780; Crawford (n 132) 37, similar also before Brownlie (n 91) 19.

[245] Hicks (n 145) 7, 41; Lepard (n 145) 166; Cheng (n 167) 23.

[246] *United States Diplomatic and Consular Staff in Tehran,* Judgment (1980) ICJ Rep 3, 86 (inviolability of diplomatic personnel and the mission).

[247] Nicaragua (n 96) 181, 188, 190 (restrain of use of force in international relations).

[248] ibid 290.

and in the *Frontier Dispute*[249] case, the ICJ referred to 'principles of customary law', *quasi* combining the general principles of international law and international customary law. Finally, the Court also referred to 'general or customary international law' in the *North Sea Continental Shelf*[250] case and ambiguously to 'general international law' in the *Barcelona Traction*[251] and *Hostages*[252] case, thus not making any difference between general principles of international law and international customary law. All in all, it might be wise to concur with those who claim that any intent of a rigid categorisation of general principles of international law would be inappropriate.[253] Depending on the content and use of a principle, it can be part of customary law or a separate and substantive source in itself.[254]

General principles of international law can also present legal rights and obligations.[255] Whereas in national law a distinction is made between a law source as objective law on the one hand and a right, an obligation or subjective entitlement on the other hand, the two aspects merge in international law due to lack of a centralised legislator.[256] In the international law system, the community of its subjects, i.e., primarily States, create the legal bonds and are subject to them at the same time.[257] Additionally, general principles as endorsed in Article 2 of the UN Charter entail directly legal rights and obligations on the basis of the binding character of contractual law.[258] However, it could be argued that a general principle of international law will achieve the quality of a right or obligation only after a specific interpretation of its general content in a concrete situation, making it thereby 'operational' in legal sense.[259] Consequently, the general principles of international law as pertaining to international peace and security would unfold their nature as a State's 'hard law' obligation in the cyber realm only after a respective interpretation and thus concretisation of the principle with regard to governmental cyber activities.

[249] Frontier Dispute (n 213) 21.

[250] North Sea Continental Shelf (n 142) 37.

[251] *Case Concerning the Barcelona Traction, Light and Power Company, Limited,* Judgment (1979) ICJ Rep 3, para 34, 87 ('body of general international law' 'guaranteed by general international law, in the absence of a treaty applicable to the particular case').

[252] Hostages Case (n 246) 62 ('obligations under general international law').

[253] Crawford (n 132) 37; Hicks (n 145) 11.

[254] Hicks (n 145) 11; Tammes (n 133) 374.

[255] Kolb (n 146) 11; Wolfrum (n 120) 34 (stating that international and regional courts and tribunals make use of principles as an interpretative tool or as a source of concrete obligations).

[256] Kolb (n 146) 11.

[257] ibid.

[258] Wolfrum (n 158) 7; Pierre d'Argent and Nadine Susani, 'United Nations, Purposes and Principles' in MPEPIL (n 1) MN 20.

[259] Similarly d'Argent and Susani (n 258) MN 20 (with regard to principles enshrined in Article 2 of the UN Charter).

5.1.3. Distinctive Status within the International Law System

General principles of international law are attributed a distinctive status within the international law system, which is, however, based on different approaches to legal reasoning and to international law.

5.1.3.1. Relationship to Opinio Iuris, Practice and Consent of States

It is widely recognised within scholarly writings that the development or recognition of general principles of international law either does not require proof of their existence, or exists independently from the consent or will of the States.

Based on the consensual approach to international law (i.e., emphasising the importance of the will of the States, who are the primary subjects creating international law), and on the presumption of general principles of international law being part of international custom, some scholars assert that the existence of the general principles is based on the States' *opinio iuris*, which, however, does not require to be evidenced.[260] They affirm that there would be an agreement within the international community that the general principles of international law have been so long and generally accepted and are still believed to be desirable, so there would be no need for an evidence of State practice for their recognition.[261] This approach corresponds with the classical theory of international custom, which perceives State practice not as a normative requirement, but as a means to proving the existence of consent (in the meaning of a tacit treaty).[262] In the case of general principles of international law, such a (tacit) consent or will of the States is presumed.[263]

However, such presumed (tacit) consent or will of the States could also be deemed irrelevant. The above-presented view is based on the notion that the existence of general principles of international law is based on the *opinio iuris* of the States. It is noted within scholarly writings that *opinio iuris* is an opinion, conviction, or belief referring to the legality or illegality of a certain behaviour of a State, thus not depending on the will of the State.[264] It is rather based on a meta-legal notion or on general legal considerations that a certain

[260] eg Brownlie (n 91) 19; Heintschel von Heinegg (n 124) § 16 MN 43; Crawford (n 132) 37; Petersen (n 145) 277 and 285; Wolfrum (n 120) 35; Hicks (n 145) 7-11; Lepard (n 145) 166.

[261] cf Brownlie (n 91) 19; Heintschel von Heinegg (n 124) § 16 MN 43; Crawford (n 132) 37; Lepard (n 145) 166.

[262] Petersen (n 145) 294ff, 300.

[263] Martti Koskenniemi, 'The Politics of International Law' (1990) 1 European Journal of International Law (4) 20-27 (claiming the binding character of general principles of international law and other non-consensual general law because of a 'subjective value of "justice"').

[264] Treves (n 141) 9.

State's conduct is just, fair or reasonable and, for that reason, required under law.[265] Thus, *opinio iuris* is based on a value judgement.[266] General principles of international law, reflecting a genuine morality and most basic values of the international society as inherent to the international order (para. 5.1.), would consequently not depend on the (tacit) consent or will (evidenced by State practice) for the proof of their existence.

Furthermore, it is asserted that general principles of international law exist independently of the practice, consent or will of the States, because they form the 'backbone' of the international law system.[267] As the international law system is an accepted reality of the international structure and order, and gives the States the platform to exercise their will, its very existence does not need consent or expression of will by the States.[268] This finding is confirmed by the ICJ, which held in the *Gulf of Maine* case:

> '[...] customary international law [...] in fact comprises a *limited set of norms for ensuring the co-existence and vital co-operation* of the members of the international community, together with a set of customary rules whose presence in the opinio juris of States can be tested by induction based on the analysis of a sufficiently extensive and convincing practice, and not by deduction from *preconceived ideas*. […]'[269]

The Court thus distinguished within the customary law a category of 'a limited set of norms for ensuring the co-existence and vital co-operation' of States deducted from 'preconceived ideas', and not from *opinio iuris*, practice, or any other form of consent or expression of the will of States.

Thus, the binding nature of general principles of international law is based either on the assumption of a tacit consent or will of the subjects of international law, i.e., primarily States, or on the notion that the general principles reflect universally accepted meta-legal principles (justice, equity and fairness).[270] This statement reflects the dichotomy of the consensual approach (recognising that international customary and contractual law is firmly based on the States' consent) and a rather natural law approach to international law. This legal dichotomy, which, at first sight, appears to be of academic value only, is especially important in the context of general principles of international law, as some of them, according to jurisprudence of the ICJ and scholarly opinion, are derived from 'preconceived ideas' and apply regardless of the States' *opinio iuris*, practice or other expressions of State consent or will.

---

[265] Wolfrum (n 120) 25; similar Koskenniemi (n 263).

[266] Wolfrum (n 120) 25.

[267] ibid; Treves (n 141) 9; Hicks (n 145) 9.

[268] cf Hicks (n 145) 9.

[269] *Case Concerning Delimitation of the Maritime Boundary in the Gulf of Maine Area,* Judgment (1984) ICJ Rep 246, para 111 [emphasis by the author].

[270] Wolfrum (n 120) 3.

This results in a most significant consequence: States cannot 'opt-out' from general principles of law that are necessary for the 'co-existence and vital co-operation' within the international community. It can be asserted that such principles are reflected by the general principles of international law as pertaining to international peace and security as identified above (para. 5.1.1.). After a respective interpretation and concretisation with regard to the cyber realm, as will be provided *infra*, they ought to be observed by States regardless of their *opinio iuris*, practice, consent or any other expression of will.

5.1.3.2. Higher 'Normative Value'

General principles of international law were described by scholars as 'so fundamental [...] that no reasonable form of co-existence is possible without their being generally recognized as valid', as 'manifestations of the universal legal conscience', or as 'principles that constitute unformulated reservoir of basic legal concepts [...], which form the irreducible essence of all legal systems'.[271] Not surprisingly, advocates of the constitutionalist approach to international law attribute general principles that are essential for the existence of the present order structure a *quasi*-constitutional role within the international law system.[272] Such principles would be, e.g., good faith, proportionality, unjust enrichment, self-determination of peoples, non-use of force, and peaceful settlement of disputes.[273] The constitutionalist approach distinguishes such 'constitutional norms' from other norms of international law and pronounces a priority of values which shall reflect a hierarchy of norms.[274] The respective debates are characterised by controversy that can be related to diverging underlying conceptions of the relationship between morality and international law.[275]

Independently from the constitutionalist approach, some authors also claim that certain fundamental principles of international law would in theory present a superior source of law.[276] This view is based on the notion, that such basic principles would be applied for the purpose of modifying and superseding conventional and customary rules, as the principles would, due to their general character and value-based content, present the standard for testing the conformity of other norms with the existing legal basis.[277] For the same reasons, they could not be overridden by any other individual rule, however specific and enacted in formal fashion.[278]

---

[271] Bassiouni (n 144) 771 (with further references).

[272] Kolb (n 146) 9, 25 and 36 ('The law of general principles is constitutional law in the fullest sense of the word. It is placed on the level of sources, of development of the law, of essential metabolistic functions within the legal order.').

[273] ibid 25ff.

[274] Venzke and von Bernstorff (n 236) 17.

[275] ibid.

[276] Cheng (n 167) 22; Bassiouni (n 144) 787; Martti Koskenniemi, 'Hierarchy in International Law: A Sketch' (1997) 8 European Journal of International Law 577; Hicks (n 145) 29: Wolfrum (n 120) 11.

[277] Hicks (n 145) 29; Bassiouni (n 144) 787.

[278] Koskenniemi (n 276) 577.

A formal hierarchy between the sources of international law must be rejected.[279] The informal hierarchy in the techniques of legal reasoning (i.e., successive orders of consideration based on ease of proof or on the approach to applicable law, proceeding from more specific to more general norms) does not introduce a hierarchy of norms.[280] Also the UN Charter, enshrining some of general principles of international law (para. 5.1.1.), cannot be viewed as a constitution or basic norm of international society at a higher normative level. The Charter is an international treaty, which according to its Article 103, prevails only over contrasting contractual obligations taken by a UN member State.

Furthermore, it is asserted that a 'heightened normativity' of certain general principles of international law could be derived from their character as peremptory norms (*ius cogens*) of international customary law.[281] The notion of *ius cogens* was first proposed by (natural law) scholars in the 17th and 18th century and was adopted in the *Vienna Convention on the Law of Treaties* (VCLT) of 1969.[282] According to Article 53 VCLT, *ius cogens* is '[...] a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character.' Given that norms, which are 'accepted and recognized by the international community of States as a whole' are based on the consent, or at least acquiescence, of the world, the *ius cogens* concept is based on the consensual foundation and not on the notion of a gateway of meta-legal or general considerations (as envisioned by the naturalists).[283] Though, *ius cogens* also indicates a certain recognition of a 'public order of the international community' based on the consensus concerning fundamental values which are not at the disposal of the subjects of that legal order.[284] Despite this distinctive nature, and in contrast to some assertions within scholarly writings,[285] *ius cogens* is not a higher category of formal sources of international law, but a particular quality of customary law norms.[286] This particular quality is not depicted by a hierarchical position, but by special consequences of the breach of the norms, as stated in Article 53 VCLT with regard to contracts and in Articles 40 and 41 of the ILC *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (referring to 'serious breach[es] by a State of an obligation arising under a peremptory norm of general international law'). Thus, it can be concluded, that, although there is no hierarchy among the sources of law, there is a notion that *ius cogens*, because of its fundamental content, is one way or another intrinsically 'superior' to all other norms.[287]

[279] Cheng (n 167) 22ff; Pellet (n 135) 265 and 268; ILC (n 110) 463 (see also 85 for more detailed information).

[280] Koskenniemi (n 276) 566-582; ILC (n 110) 463.

[281] Brownlie (n 91) 19; Crawford (n 132) 37; Bassiouni (n 144) 780.

[282] Wolfrum (n 120) 49; Jochen A Frowein, 'Ius Cogens' in MPEPIL (n 1) MN ; ILC (n 110) 361.

[283] Wolfrum (n 120) 49.

[284] Frowein (n 282) 3, 11.

[285] Cheng (n 167) 22; Wolfrum (n 120) 11.

[286] Pellet (n 135) 279.

[287] ibid 280.

Scholars are in disagreement as to what constitutes *ius cogens* and how a given rule, norm or principle rises to that level.[288] Significant State practice, which could support the identification of specific peremptory norms, has not developed.[289] Nonetheless, it is asserted that fundamental general principles of international law have the character of *ius cogens* (and are even 'merely a semantic variation'[290] of them).[291] This is based on the understanding of fundamental principles of international law as norms 'whose perceived importance, based on certain values and interests, rises to a level which is acknowledged to be superior, and thus capable of overriding another norm, rule, or principle in a given instance'.[292] This view could be deemed as confirmed by the ICJ, which stated in the *Nicaragua*[293] case 'that […] the customary international law flow[s] from a […] fundamental principle outlawing the use of force in international relations', i.e., a prohibition which is widely acknowledged as a *ius cogens* norm.

Thus, fundamental principles of international law can be attributed a 'higher normative value' – without introducing a formal hierarchy into the sources of international law – either because of their *quasi*-constitutional role within the international law system, or as peremptory norms of international custom. Taking either approach, there seems to be an understanding within the academia and within the rulings of international courts that the fundamental principles of international law do have a non-derogative character. This, as mentioned above, results in the finding that all States' behaviour has to be guided by the general principles of international law, and, whenever they also show a normative character in terms of a legal obligation, States cannot 'opt-out' from fundamental principles of international law, i.e., those which are essential for the 'co-existence and vital co-operation of the members of the international community'. This finding shows significance for fundamental principles as pertaining to international peace and security in cyberspace, as they will show a 'normative value' higher than other obligations deriving from international law.

5.1.3.3. Relationship to the Concept of Fundamental Rights and Duties of States

A different theoretical approach to the phenomenon of a 'higher normative value' of the fundamental principles of international law is given by the concept of fundamental rights and duties of States.

---

[288] Bassiouni (n 144) 801ff (with further references). In its Commentary to the *Draft Articles on State Responsibility* of 2001, the ILC gave as examples of peremptory norms the prohibition of aggression, of slavery and slave trade, of genocide, racial discrimination and apartheid, of torture, as well as basic rules of international humanitarian law applicable in armed conflict, and the right to self-determination, see ILC, *Draft Articles on State Responsibility* UN Doc 56/10, commentary on Article 40, para 4-6. In scholarly writings also the right to self-defence and the prohibition of piracy are frequently qualified as *ius cogens,* cf ILC (n 110) 374 (with a multitude of further references in footnote 522).

[289] Wolfrum (n 120) 50.

[290] Bassiouni (n 144) 780.

[291] ibid; Brownlie (n 91) 19; Crawford (n 132) 37.

[292] Bassiouni (n 144) 805.

[293] Nicaragua (n 96) 181, 188, 190 (refrain from the use of force in international relations).

The doctrine emerged in the 17th century (coinciding with the Peace of Westphalia of 1648, marking the beginning of modern international law) and is based on the independence (from papacy and empire) and equal sovereignty of States (with regard to their exclusive dominion of territorial jurisdiction).[294] According to the concept, the existence of fundamental rights and duties is inherent to the essence of a State.[295] The specification of the nature of such fundamental rights and duties is problematic, as pursuant to the doctrine, they would constitute a *quasi*-constitutional basis, upon which all other international law norms are based.[296]

At the beginning of the 20th century (and especially on the American continents) several inter-governmental conferences dealing with fundamental rights and duties of States were conducted, resulting in respective political declarations.[297] Additionally, diverse international lawyers associations developed declarations of fundamental rights and duties of States.[298] Also, several international treaties codifying States' views on fundamental rights and duties were concluded.[299] In 1949, the ILC elaborated (upon request of UNGA)[300] a draft *Declaration on the Rights and Duties of States*[301] containing 14 articles, which was transmitted by UNGA to States for considerations on further action. However, already within the ILC the draft was voted against only by the US and the USSR, and States never requested UNGA to take the issue up again.[302] It should be mentioned that, according to the draft's preparatory work, the ILC considered Article 2 of the UN Charter as expressing fundamental rights and duties of States.[303] In the same line, the *Friendly Relations Declaration* could be seen at the first sight as reflecting fundamental rights and duties of States.[304] However,

[294] Sergio M Carbone and Lorenzo Schiano de Pepe, 'States, Fundamental Rights and Duties' in MPEPIL (n 1) MN 3; ILC (n 105) 1-4.

[295] Carbone and Schiano de Pepe (n 294) MN 1 and 30; Volker Epping and Christian Gloria, 'Der Staat im Völkerrecht' in Ipsen (n 124) § 26 MN 1.

[296] Epping and Gloria (n 295) § 26 MN 2.

[297] eg *Declaration of American Principles of the Eights International Conference of American States* of 1938. For more information see ILC (n 110) 149-153.

[298] eg American Institute of International Law in 1916 (*Declaration of Rights and Duties of Nations*); the International Juridical Union in 1919 (*Draft of a Declaration of Rights and Duties of Nations*); the International Commission of American Jurists in 1927 (Report *Project II, States: Existence, Equality, Recognition*); the Union Juridique International/International Law Association in 1936, or the Inter-American Juridical Committee in 1942 (*Reaffirmation of Fundamental Principles of International Law*). For more information see Carbone and Schiano de Pepe (n 294) 6; ILC (n 110) 156ff.

[299] eg the *(Montevideo) Convention on Rights and Duties of States* (inter-American) of 26 December 1933; the *Charter of Organization of American States* of 30 April 1948 (Chapter IV), or the *Charter of the Organization of African Unity* of 25 May 1963 (Article III and V; abrogated in 2000 by the *Constitutive Act of the African Union*). Article III of the OAU Charter (*Principles*) referred to sovereign equality, non-interference, peaceful settlement of disputes; Article V (*Rights and Duties of Member States*) referred to equal 'rights and duties of Member States'.

[300] UNGA Res 178 (II) (21 November 1947) para 3.

[301] UNGA Res 375 (IV) (6 December 1949) annex.

[302] Carbone and Schiano de Pepe (n 294) 14; Fassbender (n 225) 30.

[303] ILC (n 110) 140.

[304] Epping and Gloria (n 295) § 26 MN 5.

despite mentioning 'rights and duties of Member States under the [UN] Charter' (General Part, para. 2) the declaration is drafted in terms of 'basic principles' rather than of 'rights and duties' (para. 5.1.1.).

Summarising the different treaties, declarations and drafts, the catalogue of the fundamental rights and duties of States can be deemed to comprise:[305]

- equal sovereignty,
- independence,
- jurisdiction,
- non-intervention,
- restrain from (threat or) use of force,
- self-defence (also in the broader term of self-preservation),[306]
- peaceful settlement of disputes,
- mutual respect of the rights of all,
- immunity of ambassadors,
- *pacta sunt servanda*,
- good faith, and
- (respect for human rights and fundamental freedoms).[307]

Scholars have asserted the fundamental rights and duties of States as forming part of general principles of international law that aim at governing the friendly and peaceful coexistence and cooperation of States, and have described them as being objective, independent of any expression of willingness by States, particularly inalienable and absolute in nature.[308] Indeed, content-wise and with regard to the distinctive status claimed for the fundamental rights and duties, they resemble the general principles of international law that are essential for the 'co-existence and vital co-operation of the members of the international community'.

The relevance of the doctrine of fundamental rights and duties of States can be judged as minimised by the emergence of international law subjects other than States (i.e., international organisations), by the increasingly complex (contractual) interaction and interdependence of States in times of globalisation impairing their sovereignty, and perhaps

[305] The assessment is based on the texts of the aforementioned treaties and declarations, especially the draft declaration prepared by the ILC for UNGA (n 301) as well as on scholarly writings.

[306] Carbone and Schiano de Pepe (n 294) 28.

[307] eg Article 6 of the ILC draft declaration (n 301).

[308] Carbone and Schiano de Pepe (n 294) 30ff; Epping and Gloria (n 295) § 26 MN 3.

also because of its natural law ascendancy. However, their contents, i.e., the legal independence and equal sovereignty as well as the principles deriving from this basic foundation, remain crucial to the functioning of the international order.

Thus, despite the different doctrinal approach, the concept recognises the notion that some basic principles form the very foundation of the international law order. Content-wise the fundamental rights and duties of States resemble the principles identified within the scholarly writings as 'constitutional', of 'higher normativity', and those essential for the 'co-existence and vital co-operation of the members of the international community' (para. 5.1.3.2.).

5.1.4. Instrument of Progressive Law Development

General principles of international law may serve different purposes. They are a normative source of law, which governs situations not regulated by formulated norms.[309] By introducing overarching considerations into international law, they also serve as a guideline or framework for interpretation of conventional and customary international law.[310] For the same reason, they have the function of systematisation of law, in the meaning of amelioration of the fragmentation of international law.[311] However, the most important feature of general principles of international law is their function as a basis for the progressive development of international law.[312] This feature is especially interesting in the realm of international peace and security in the cyber context, as cyber specific customary law is absent and contractual regulation scarce (para. 5.).

General principles of international law have the necessary degree of abstraction and concreteness to be able to be dynamic yet filled with some specific legal meaning.[313] Their generality and flexibility enables the principles to be the means of substantial, progressive development of international law.[314] Such development can occur by progressive interpretation of international law guided by the principles, as there is (apart from relatively few exceptions) no law-application without some law-creation.[315] General principles of law may also be the starting point for the evolution of a new rule of customary law and thus play the middle role between *lex lata* and *lex ferenda*.[316] Last but not least, general principles can also serve *per se* as a basis for the development of new rights and obligations.[317] Especially in

[309] Cheng (n 167) 390; Bassiouni (n 144) 775ff; Wolfrum (n 120) 34ff; idem (n 158) 20.

[310] ibid.

[311] Wolfrum (n 158) 7 and 20.

[312] ibid.

[313] Kolb (n 146) 9.

[314] ibid; Wolfrum (n 120) 39; Bassiouni (n 144) 804.

[315] Kolb (n 146) 7-9; Wolfrum (n 120) 39.

[316] ibid.

[317] Kolb (n 146) 30; Wolfrum (n 120) 39.

the absence of relevant international practice and of applicable specific rules, the recourse to general principles of international law is the only option for not leaving a specific situation in a legal *lacuna*. Considering the inherent limitations for the modifications of treaty law as well as of customary international law, general principles of international law can be thus deemed as 'transformators' of rising extra-positive (social, moral, etc.) needs of the international community into international law by subsuming the new situation to a principle and by a deduction or reception from the principle.[318] This way, general principles of law play a prominent role in legal dynamics, in the development of the law, in the adaptation of law to new situations, and consequently in the filling of the *lacunae*.[319] They prevent a static application of archaic norms in a legal system which needs to respond to the dynamic needs of the international society, especially to meet the needs of fast growing technological advances.[320]

The development of international law by a modern interpretation of the general principles (or creation of new sub-principles) will not occur in the abstract, but as a reaction to practical needs and specific phenomena that calls for development. The 'emergence' of cyberspace and its relevance for international peace and security justifies a re-consideration of that particular body of law. Thus, the new phenomenon of cyberspace as a new common space for inter-State relations, results in the need of fundamental regulation as pertaining to the international peace and security. In this regard, a modern interpretation of the respective general principles of international law will support the progressive development of international law.

5.1.5. ntermediate Result

General principles of international law are either derived from Article 38(1)(c) of the ICJ Statute or present a separate source of international law existing beside the enumeration of that Article. Hitherto, neither international courts nor academia have developed methods for identifying the principles. By whichever methodology, general principles of international law can be derived from general considerations, legal logic, legal relations in general, international relations, or from a particular treaty regime. The international courts as well as scholars have identified several general principles of international law of contractual nature, of procedural character, or of relevance to specific situations. With regard to general principles of international law as pertaining to international peace and security, international courts and academia have acknowledged the existence of the following principles:

- sovereign equality of States, including the correlated principles of:
    - self-preservation,
    - independence,

[318] Wolfrum (n 158) 60.

[319] Kolb (n 146) 30.

[320] Bassiouni (n 144) 777ff.

    - jurisdiction over domestic matters,
    - non-intervention in matters within the domestic jurisdiction of other States,
    - duty not to harm the rights of other States,
- maintenance of international peace and security, including the principles of:
    - restrain from (threat or) use of force in international relations,
    - duty to peaceful settlement of disputes,
- duty to international cooperation in solving international problems.

These principles are endorsed in Article 1 and 2 of the UN Charter and confirmed by the UNGA *Friendly Relations Declaration*, as well as, e.g., by the *Helsinki Declaration*.

Despite their generality and the value-based differences within the international community, general principles of international law are recognised as a normative source of law, either as part of international customary law or as a separate source of international law. Following a specification of their contents by an interpretation in a concrete situation, general principles of international law achieve the quality of a 'hard law' obligation or of a right of a State.

Due to their nature as the foundation of the international law system, it is widely recognised within scholarly writings that general principles of international law that are essential for the 'co-existence and vital co-operation of the members of the international community' exist irrespective of State's *opinio juris* practice, consent or any other expression of the will of a State. Moreover, such principles enjoy a 'heightened normativity' – without introducing a formal hierarchy to the sources of international law – because of their *quasi*-constitutional role within the international law system or as peremptory norms of international custom. This finding is also recognised by the doctrine of fundamental rights and duties of States, which attributes such principles to be inherent to the essence of a State. This results in the utmost important finding that States cannot 'opt-out' from general principles of law that are necessary for the 'co-existence and vital co-operation' within the international community.

General principles of international law may serve different purposes, of which the most significant is the function as a basis for the progressive development of international law (either by filling a legal *lacuna* or by progressive interpretation of existing international norms), responding to rising extra-positive needs of the international society, such as fast growing technical advances, e.g., the 'emergence' of cyberspace as a common space for inter-State relations.

5.2. Specific General Principles of International Law Applicable to Cyberspace

CBMs, as recommended by or proposed during the current negotiations in the international fora or as expressed in bilateral agreements and in unilateral declarations (para. 3.3.), reflect the views of the (participating) States as to which conduct is deemed as politically acceptable or even required. In terms of the significance of political declarations for the development of international law, perhaps even in form of 'soft law' (para. 4.), they can serve as guidance for the interpretation of those general principles of international law, which are relevant to international peace and security (see enumeration at para. 5.1.1.). After a respective concretisation in the context of cyberspace, these general principles of international law achieve the quality of legal ('hard law') obligations of States. Furthermore, as general principles pertaining to international peace and security can be regarded as necessary for the 'co-existence and vital co-operation' within the international community, they will apply irrespective the States' practice, *opinio iuris*, consent or will, and show a 'heightened' normativity from which States cannot decline (para. 5.1.3.).

5.2.1. Sovereign Equality of States and Corollary Principles

Sovereignty is the core notion of statehood and the axiomatic principle on which, in the words of the ICJ,[321] 'the whole of international law rests'.[322] It can be asserted that most, if not all principles of international law directly or indirectly rely on State sovereignty.[323] The principle is endorsed in Article 2(1) of the UN Charter in the form of an adjective ('sovereign equality') and ensures the juridical (not geographic, economic, military, demographic, political or other) equality of States.[324]

The understanding of sovereignty has undergone changes since its formal establishment in the Peace of Westphalia in 1648. Especially since 1945, its impact has been impaired by the recognition of international organisations as subjects of international law (approximately 7,000) and the acknowledgment of their decisions as a potential sources of international law, by globalisation, the growing interdependence of States, and subsequent extended cooperation in fields which were formerly considered as domestic matters (approximately 50,000 international treaties are registered with the UN), by the recognition of rights of peoples (self-determination) as well as of individuals before specific international courts.[325] Furthermore, the notion of sovereignty is impaired by the understanding that States are

[321] Nicaragua (n 96) 263.

[322] cf Brownlie (n 91) 287; Heintschel von Heinegg (n 124) § 16 MN 43; Crawford (n 132) 447; Juliane Kokott, 'States, Sovereign Equality' in MPEPIL (n 1) MN 1.

[323] Samantha Besson, 'Sovereignty' in MPEPIL (n 1) MN 2; cf Epping and Gloria (n 295) § 26 MN 13.

[324] d'Argent and Susani (n 258) 11.

[325] cf Besson (n 323) 3-55, 153; Kokott (n 322) 79, 27; Bardo Fassbender, 'Die Souveränität des Staates als Autonomie im Rahmen der völkerrechtlichen Verfassung' in Heinz-Peter Mansel et al. (ed), *Festschrift für Erik Jayme* (vol 2, Sellier 2004) 1093ff, idem (n 225) 69ff.

obliged to promote and safeguard common values and goals of the international community.[326]

This is especially true with regard to cyberspace. The internet developed into a global network by a bottom-up, distributed efforts of mainly private stakeholders. Cyberspace (see definition in para. 1), including its 'global public memory', is mainly driven by the civil society. The Westphalian elements of international order, of horizontal, inter-State relations (emphasising the States as primary subjects of international law) are complemented in cyberspace in an extensive way by aspects of political, economic and social networks, characterised by vertical and diagonal linkages between governments, (transnational) companies, peoples, societies and individuals. The Internet Corporation for Assigned Names and Numbers (ICANN),[327] the non-governmental organisation (NGO) 'governing' the internet, can be deemed as reflecting this notion, as it takes an internationalised and multi-stakeholder approach to its operation.

Yet, although flexibly changing its nature, State sovereignty is still the foremost principle of international law and shows several significant facets and corollary principles, which will be presented in the following as applicable to cyberspace.

5.2.1.1. Self-Preservation

One of the corollary principles of equal sovereignty is a State's right to self-preservation. In its *Nuclear Weapons*[328] advisory opinion, the ICJ recognised 'the fundamental right of every State to survival, and thus its right to resort to self-defence, in accordance with Article 51 of the Charter, when its survival is at stake'. A right to self-defence is given in situations of an 'armed attack' launched by another State (or possibly by non-State actors), entitling the victim State to use defensive military force (Article 51 of the UN Charter and corresponding international custom[329]). Currently, neither a legal definition nor a universally accepted

[326] Fassbender (n 325) 1095.

[327] ICANN is a Californian (US) non-profit, public benefit corporation, which, in the framework of a Public Private Partnership, acts on behalf of and reports to the US Department of Commerce (however, the organisation emphasises its international nature and independence). ICANN bears global responsibility for ensuring the stable and secure operation of the internet as well as for coordinating the internet system of unique identifiers, i.e., for the assignment of IP address ranges (since 2005 to regional organisations). It is further responsible for the generic codes and country codes of the internet top level domain as well as for the management and maintenance of the 127 internet root servers (which of location is secret), which is the foundation of the internet. ICANN is contracted by the US Department of Commerce to perform the functions of the Internet Assigned Numbers Authority (IANA), which was executing the above-mentioned tasks directly on behalf of the US Department of Commerce. See ICANN, Factsheet <http://archive.icann.org/en/factsheets/fact-sheet.html>; ICANN/US Department of Commerce Contracts on IANA Functions <http://www.icann.org/en/about/agreements>.

[328] Nuclear Weapons (n 103) 96.

[329] Albrecht Randelzhofer and Georg Nolte, 'Article 51' in Simma (n 223) MN 10-12 (with further references); Karl Zemanek, 'Armed Attack' in MPEPIL (n 1) 14-21; Christopher Greenwood, 'Self-Defence' in MPEPIL (n 1) 1; Yoram Dinstein, *War, Aggression and Self-Defence* (3rd edn, Cambridge 2001) 165; Ian Brownlie, 'International Law and the Use of Force by States Revised' (2000) 21 Australian Yearbook of International Law 26; Brownlie (n 91) 272-275.

definition of the term 'armed attack' exists. It should be mentioned that State practice with regard to 'armed attacks' in the cyber context is not detectable and States prefer to maintain a strategic ambiguity with regard to the question as to under which circumstances they would consider malicious cyber activities as an 'armed attack', which leaves the respective discourse to academia.

In general terms, according to the ICJ and to scholarly writings, the notion of an 'armed attack' does not imply the use of specific weaponry, and can be thus conducted, for example, by electronic means.[330] Although disputed in detail, it can be asserted that an 'armed attack' is given in most severe cases of 'use of force' in international relations (Article 2(4) of the UN Charter) of significant scale and effects. This finding is supported by the jurisprudence of the ICJ[331] as well as by a vast amount of scholarly writings.[332] Thus, the question whether a situation of an 'armed attack' is given depends on the assessment, whether a certain behaviour and their effects can be deemed as 'use of force' in the meaning of Article 2(4) of the UN Charter – a question which will be dealt with *infra* with regard to malicious cyber activities (para. 5.2.2.1.).

As cyberspace enables (skill and knowledge-wise) super-empowered individuals to cause severe physical effects through manipulations of computer systems that the functioning of highly developed post-industrial States depends upon, the question arises whether they can trigger the right to self-defence. There are considerable pros and cons, the demonstration of which would exceed the scope of this paper.[333] In addition, the value of the so-called 'safe haven' theory,[334] developed in the context of self-defence with regard to terrorists acting from the territory of States unwilling or unable ('failed States') to impede activities of non-State actors harmful to other States, should be considered in the context of State responsibility for malicious cyber activities conducted by non-State actors otherwise qualifying as 'armed attack'. In this context, it would surely be beneficial to further discuss,

[330] Randelzhofer and Nolte (n 329) 43; Zemanek (n 329) 21; Nuclear Weapons (n 103) 39.

[331] cf Nicaragua (n 96) 191, 195 ('the most grave forms', '[…] of significant scale […]', '[…] because of its scale and effects, would have been classified as an armed attack rather than a mere frontier incident […]'); Oil Platforms (n 100) 51, 64 and 72. With regard to the lawfulness of the use of armed force in cases of 'low intensity conflicts', see Randelzhofer and Nolte (n 329) 8.

[332] cf Randelzhofer and Nolte (n 329) 4ff. and 20; Zemanek (n 329) 7; Greenwood (n 329) 12; Michael Bothe, 'Völkerrechtliche Verhinderung von Gewalt (*ius contra bellum*)' in Wolfgang Graf Vitzthum (ed), *Völkerrecht* (De Gruyter 2001) section 8 para 10; Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford University Press 1994) 250.

[333] cf eg Zemanek (n 329) 14-21; Michael N Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revised' (2011) 56 Villanova Law Review 600ff; Katharina Ziolkowski, *Gerechtigkeitspostulate als Rechtfertigung von Kriegen. Zum Einfluss moderner Konzepte des Gerechten Krieges auf die völkerrechtliche Zulässigkeit zwischenstaatlicher Gewaltanwendung nach 1945* (NOMOS 2008) 221-229, demonstrating the lines of interpretation of Article 51 of the UN Charter, of the respective international customary law, as well as of international courts' jurisprudence, State practice and resolution practice of UN organs after the events of 9 September 2001. The Netherlands confirmed their view that non-State actors can conduct an 'armed attack' in cyberspace, see The Netherlands, 'Government response to the AIV/CAVV report on cyber warfare' (Statement of 17 January 2012) 5 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf>.

[334] For an overview on the major lines of argumentation, see Schmitt (n 333) 602ff.

e.g., the criteria of the terms 'unable' and 'unwilling' and the authority to determine their presentation in a concrete case. An academic and political discourse on the aforementioned matters can probably not be avoided in the future.

Very likely, cases of preventive self-defence, i.e., in situations of an immediate 'armed attack', when '[…] the necessity of self-defence is instant, overwhelming, leaving no choice of means, and no moment for deliberation.',[335] will stay theoretical. This is based on the fact that, despite potential additional intelligence, the intended effect of malicious cyber activities will not be visible beforehand. Moreover, judged from today's perspective, even in the case of discovery of malicious codes in, for example, governmental computer networks, there still would be a 'choice of means' and a 'moment for deliberation'. Malware can be isolated, penetrated networks disconnected and IT security measures directed at the affected networks. Additionally, the concept of 'pre-emptive' (anticipatory) self-defence was asserted by some scholars, namely in the case of the implementation of the computer worm Stuxnet to Iranian nuclear facilities 2008-2010.[336] The concept of 'pre-emptive' self-defence, i.e., in cases of a mere suspicion of future armed attacks primarily based on mistrust towards a State's behaviour in international relations, is to be strictly refused[337] for several reasons, also regarding the specific case of Stuxnet.[338] Preventive measures against latent threats to international peace and security are within the decision-making authority of the UN Security Council (UNSC) (Article 39 of the UN Charter).

Furthermore, the 'accumulation of events' or '*Nadelstichtaktik*' theory will surely need to be considered within the cyber realm. The concept states that, in a situation of a series of incidents, of which each one classifies as 'use of [armed] force' but does not show the necessary scale and intensity qualifying it as an 'armed attack', the whole series of these occurrences would cumulatively form the basis for the assessment of the immediacy, scope and intensity. Advocates of this approach claim that a State facing a 'hit and run' tactic of

[335] So-called 'Webster formula', phrased by the US State Secretary Webster in a letter to the British government of 24 April 1837, on the occurrence of the destruction of the US ship 'Caroline'; quoted by Brownlie (n 91) 43. On the 'Caroline Case' see Christopher Greenwood, 'Caroline, The' in MPEPIL (n 1).

[336] See Michael N Schmitt (gen ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) Rule 13 para 13; contra: Katharina Ziolkowski, 'Stuxnet – Legal Considerations' (2012) 25 Journal of International Law of Peace and Armed Conflict (3) 143ff.

[337] Greenwood (n 329) 47ff; Michael Bothe, 'Terrorism and the Legality of Pre-emptive Force' (2003) 14 European Journal of International Law 230; Georg Nolte, 'Die USA und das Völkerrecht' (2003) 78 Friedens-Warte 191; Christian Tomuschat, 'Iraq – Demise of International Law?' (2003) 78 Friedens-Warte 146; Rüdiger Wolfrum, 'The Attack of September 11, 2001, the Wars Against the Taliban and Iraq: Is There a Need to Reconsider International Law on the Recourse to Force and the Rules in Armed Conflict?' (2003) 7 Max Planck Yearbook of United Nations Law 33; Ziolkowski (n 333) 235-240. See also *Case Concerning Armed Activities on the Territory of the Congo,* Judgement (2005) ICJ Rep 168, para143 and 148. Contra: Olivier Corten, 'The Controversies Over the Customary Prohibition on the Use of Force. A Methodological Debate' (2005) 16 European Journal of International Law 807; W. Michael Reisman, 'Assessing Claims to Revise the Law of War' (2003) 97 American Journal of International Law 87; Michael N Schmitt, 'Preemptive Strategies in International Law' (2003) 24 Michigan Journal of International Law 534; Abraham D Sofaer, 'On the Necessity of Pre-emption' (2003) 15 European Journal of International Law 210 and 214; Michael J. Glennon, 'The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter' (2002) 25 Harvard Journal of Law and Public Policy 552ff; Dinstein (n 324) 220.

[338] cf Ziolkowski (n 336) 143ff.

another State would have no other choice but to undertake military measures to counter it.[339] In the past, the concept was invoked by Israel (*Nadelstichtaktik*)[340] to justify the use of military force against terrorist groups located on the sovereign territory of its neighbouring States.[341] Furthermore, the US made use of the concept (accumulations of events theory),[342] e.g., to justify the bombardment of specific sites in Sudan and Afghanistan on 20-21 August 1998 in a letter to the UNSC, stating:

> 'These attacks were carried out only after repeated efforts to convince the Governments of the Sudan and the Taliban regime in Afghanistan to shut these terrorist activities down and to cease their cooperation with Bin Ladin's organization. That organization has issued a series of blatant warnings that 'strikes will continue from everywhere' against American targets […]. The United States, therefore, had no choice but to use armed force to *prevent these attacks from continuing*. In doing so, the United States has acted pursuant to the *right of self-defence* confirmed by Article 51 of the Charter of the United Nations.'[343]

Along these lines, some US and United Kingdom (UK) scholars view terrorist activities against the US as a continuous process.[344] Consequently, these scholars affirm that, due to the cumulative assessment of all terrorist activities, immediacy as well as a sufficient scope and intensity of an 'armed attack' is given at any time. Interestingly, the UNSC, including the US as a veto-power, clearly refused the rationale of the 'accumulation of events theory' by condemning on several occasions (until the 1970s) military actions justified on the basis of that theory (partly explicitly referring to the acts as 'retaliation').[345] On the contrary, the judgments of the ICJ in the *Nicaragua*[346] and *Oil Platforms*[347] cases indicate that the Court accepted the theory in general. However, the concept should be approached with caution. In

---

[339] Dietrich Schindler and Kay Hailbronner, *Die Grenzen des völkerrechtlichen Gewaltverbots* (CF Müller 1986) 84; cf Nicaragua (n 96) 231 ('[…] incursions [...] amounting, singly or collectively, to an armed attack […]').

[340] The term is used, eg, by Yehuda Zvi Blum, 'The Legality of State Response to Acts of Terrorism', in Benjamin Netanyahu (ed), *Terrorism. How the West Can Win* (Farrar, Straus and Giroux 1986) 135.

[341] Constantine Antonopoulos, *The Unilateral Use of Force by States in International Law* (A. Sakkoulas 1997) 75.

[342] Used first by the UNSC in 1953 during a meeting on military actions conducted by Israel against Libya, cf UN/SCOR 8th year, 637th meeting, para 4.

[343] UN Doc S/1998/780 (20 August 1998) [emphasis by the author].

[344] cf Ruth Wedgwood, 'Responding to Terrorism: The Strikes Against bin Laden' (1999) 24 Yale Journal of International Law 564; Christopher Greenwood, 'International Law and the "War Against Terrorism"' (2002) 78 International Affairs 312; Rein Müllerson, '*Ius ad bellum* Plus Ca Change (de Monde) Plus C´est la M´me Chose (le Droit)?' (2002) 7 Journal of Conflict and Security Law 149ff; Sienho Yee, 'The Potential Impact of the Possible US Responses to the 9-11 Atrocities on the Law regarding the Use of Force and Self-Defence' (2002) 1 Chinese Journal of International Law 292.

[345] cf UNSC Res 101 (1953) (24 November 1953) part B para 1 and part A para 1 (Israel against Jordan); Res 111 (1956) (19 January 1956) preamble para 4, para 3 and 6 (Israel against Syria); Res 188 (1964) (9 April 1964) para 1 and 3 (UK against Arabic Republic Yemen); Res 265 (1969) (1 April 1965) preamble para 4, para 3 (Israel against Jordan).

[346] Nicaragua (n 96) 146.

[347] Oil Platforms (n 100) 64.

the cyber context, only malicious cyber activities qualifying as 'use of [armed] force', and which – upon reliable information – will be followed with the utmost probability by other malicious cyber activities of the same quality, can be deemed as cumulatively amounting to an 'armed attack'.

Additionally, it can be asserted that the fundamental right of States to self-preservation also entails the right to take protective measures in situations of necessity. Necessity is given when essential interests of a State (or possibly of the international community as whole) are facing grave and imminent peril.[348] Under strict conditions, States may safeguard such interests by taking protective measures (see Article 25 ILC *Draft Articles on Responsibility of States for Internationally Wrongful Acts*).

It should be mentioned that the usual expectation of defence measures being conducted by a State's armed forces will probably not be met in the pure cyber context. Armed forces must develop and maintain defensive cyber capabilities in order to be able to defend their own networks (including the deployable components thereof), and thus to ensure their operability. They should develop offensive cyber capabilities as an additional military capability, enhancing the potential of precise, potentially non-lethal possibilities of interruption and disruption without necessarily causing physical damage outside of the targeted computer networks, i.e., to living beings or to objects. However, malicious cyber activities of a level which could be deemed as an 'armed attack' against a State will probably target critical infrastructure systems which, in technologically advanced States, are highly dependent on the availability and integrity of ICTs, and which are majority privately owned. In the case of a cyber 'armed attack' in the meaning of Article 51 of the UN Charter, e.g., against the banking system as such or the energy generation and distribution systems, only the ISPs will notice irregular data streams (through monitoring of their network traffic sensors collecting information about the 'net flow', i.e., amount of routed data) and only the CERTs of the respective private companies will notice infections by malicious software (by monitoring of the intrusion detection/prevention systems conducting deep package filtering or by indications of malfunctioning of the facility's operations). At the same time, only these ISPs and CERTs will be able to deter such 'attacks' on a 'bit for byte' basis, as only they will have the possibility to block data streams or to undertake infection recovery activities based on the knowledge of the specific architecture, operating systems and adjustments the targeted complex computer systems show. Additionally, the defence of the actual 'armed attack' conducted by cyber means will most probably require recourse to the possibilities and capabilities of private cyber security companies providing 'patches' for the targeted software or of companies which developed the targeted, specific, industrial IT systems or software. This will leave the actual conduct of the 'bit for byte' cyber defence measures to the economy, i.e., to the civil society as opposed to armed forces. The armed forces and other governmental entities can only support the economy in such endeavours, for example, by providing intelligence or other forms of assistance (apart from conducting measures such as kinetic defence to deter the armed attack). One of the consequences could be that, according to Article 51(3) of the Additional Protocol I of 1977 to the Geneva Conventions of

[348] See Ziolkowski (n 333) 285-331 on 'necessity' as a general principle of international law, which might exceed the notion of Article 25 ILC draft articles on *Responsibility of States for Internationally Wrongful Acts*.

1949 (and respective customary law), the acting ISP and CERT personnel could lose the protection civilians enjoy against direct attack and become a legitimate military target (for the duration of actively defending the attacked networks). The existence of a (paramilitary) Estonian Defence League's Cyber Unit, the Austrian idea of 'voluntary cyber fire-brigades',[349] and respective considerations as currently addressed in Latvia reflect the endeavours of States to link private defence capabilities to the government.

Interestingly, the sets of (draft) CBMs do not reflect the above-mentioned aspects related to self-defence (or necessity). Although States in general prefer to maintain a strategic ambiguity with regard to questions relating to armed attack (and consequently: use of force), thus leaving the debate to academia, it would certainly support predictability and stability in international relations, if they shared their views on these matters.

5.2.1.2. Territorial Sovereignty and Jurisdiction

Another principle corollary to equal sovereignty of States is the principle of territorial sovereignty, including the principle of jurisdiction.

The aspect of territorial sovereignty, i.e., the exercise of full and exclusive authority over a territory, protects physical components of the internet ('cyber infrastructure') that are located on a State's territory or are otherwise under its exclusive jurisdiction.[350] This includes any technical and other physical components located on the land territory, in internal waters, territorial sea, archipelagic waters, in national airspace or on platforms (e.g., vessels, aircraft or satellites).[351] On the contrary, a State cannot claim territorial sovereignty (or right to appropriation) with regard to the internet as a whole (that is, a global resource) or to cyberspace (that is, a common space).[352] Due to the global nature of the internet and cyberspace, this finding is not impaired by the fact that the internet is 'governed' by ICANN, which acts on behalf of and reports to the US Department of Commerce.

Territorial sovereignty is violated by any acts causing physical effects on another State's territory.[353] However, as indicated by the US,[354] who declared that it considered its (territorial) sovereignty as violated by 'disruption of networks and systems', i.e., including

[349] cf 'Österreich überlegt Aufstellung einer „Freiwilligen Cyberwehr"' *Der Standard* (28 June 2012) <http://derstandard.at/1339639277027/Oesterreich-ueberlegt-Aufstellung-einer-Freiwilligen-Cyberwehr>.

[350] Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in Czosseck, Ottis and Ziolkowski (n 12) 7ff, 10, 13.

[351] ibid 11.

[352] cf ibid 9.

[353] cf ibid 11ff, 16; Lawrence T. Greenberg, Seymour E Goodman and Kevin J Soo Hoo, *Information Warfare and International Law* (US National Defence University 1998) 24; similar: Christopher C. Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 European Journal of International Law 842.

[354] The President of the United States of America (n 14) [call-out-box, 'Defence Objective'].

intrusions without (directly or indirectly) showing a physical effect, it could be argued that physical damage is irrelevant in the cyber context.[355] Indeed, due to the enormous negative effects malicious cyber activities can have on the national security of another State, which can be, although not of physical nature, though well 'perceptible', it can be claimed that such effects could violate the victim State's sovereignty.

The principle of jurisdiction describes the power of a State to define and to enforce rights and duties, and to control the conduct of natural and juridical persons (primarily on its own territory).[356] A State exercises its jurisdiction by establishing rules (legislative jurisdiction), procedures for identifying breaches of the rules and the precise consequences thereof (judicial jurisdiction), and by forcibly imposing consequences (enforcement jurisdiction).[357]

The general access to the internet (or digitalised access to information) can be deemed as protected by the universal human right to seek, receive and impart information through any media (see Article 19(1) of the *International Covenant on Civil and Political Rights* of 1966; Article 10(1) of the *European Convention on Human Rights* of 1950). However, a State may regulate internet activities of its own (nationality principle) and foreign (territoriality principle) nationals in its territory (or those conducted on foreign territory but showing effects on its own territory),[358] e.g., with regard to contents of uploads or downloads, including questions of what is deemed offensive in terms of morality, culture, security and stability.[359] The fact that the components of the internet are located on a State's sovereign territory but form, at the same time, part of the global internet, does not indicate a waiver of the exercise of such territorial jurisdiction.[360]

The principle of jurisdiction would certainly be violated by law enforcement activities[361] (i.e., exercise of authority) conducted by foreign agencies in networks and computers located on its own territory and outside of a cooperation framework or otherwise without a prior consent of the territorial State (e.g., online search). Especially with regard to cybercrime law enforcement, the exercise of jurisdiction of States may overlap due to the competing territorial, personal and effects based facets of jurisdiction, additionally complicated by the mobility of users and technological advances such as cloud-based computing. These aspects call for intensified cooperation measures in cybercrime law enforcement, which are reflected by CBMs for cyberspace as recommended by the UN GGE (para. 3.3.1.), stating the need to develop 'enhanced mechanisms for law enforcement cooperation'.

[355] Similarly, in the context of territorial sovereignty Heintschel von Heinegg (n 350) 11ff.

[356] Bernard H. Oxman, 'Jurisdiction of States' in MPEPIL (n 1) MN 3.

[357] ibid.

[358] ibid 32.

[359] ibid 31; similarly Heintschel von Heinegg (n 350) 9, 14ff.

[360] cf Heintschel von Heinegg (n 350) 14.

[361] cf Oxman (n 356) 47.

5.2.1.3. Non-intervention in Domestic Affairs

A further principle deriving from the sovereign equality of States is the principle of non-intervention in the internal or foreign affairs of another State. It is endorsed in regional conventions (e.g., Articles 16-19 of the OAS, Article III(2) of the *Charter of the Organization of African Unity*), reflected in political declarations (e.g., Principle VI of the *Helsinki Final Act* of 1975), in UNGA resolutions,[362] and is endorsed in Article 2(7) of the UN Charter (with regard to UN organs). The principle is confirmed by the ICJ as a rule of international custom.[363] An illegal intervention occurs when a State interferes with the internal or external affairs of another State considered by the latter as 'internal' or 'domestic' (*domaine réservé*), in order to coerce the other into certain behaviour.[364]

In general terms, it can be asserted that *domaine réservé* describes areas not regulated by international norms or not being of some common interest or value.[365] Due to globalisation, the integration of States in international organisations, the growing interdependence and subsequent cooperation of States, and especially the myriad of conventional law, very few matters can nowadays be regarded as remaining within the limits of purely 'domestic jurisdiction'.[366] One of the matters which are still recognised as *domaine réservé*, although significantly internationalised by human rights law, is the jurisdiction over, and the regulation and treatment of own and foreign nationals.[367] So far, the deliberations as presented above apply (para. 5.2.1.2.).

The internet communication as such (as opposed to national intranets) cannot be deemed as an internal affair of a State, as international telecommunications are regulated by international law (Articles 33-48 of the ITU Constitution, e.g., with regard to denial or restriction of internet connectivity). Additionally, due to the nature of the internet as a globally shared resource and to the – in general – worldwide spread of malicious software, aspects of national cyber security, i.e., questions of the establishment of cyber security measures of a strategic, political, legal, administrative, organisational or technical nature, including the establishment of a national CERT, must be deemed as of internationalised interest or value, and thus outside of the realm of purely internal affairs.

---

[362] eg *Friendly Relations Declaration* (n 224) Principle 1; *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty* UNGA Res 2131 (XX) (21 December 1965) para 2; *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States* UNGA Res 36/103 (9 December 1981) para 2, Principle I(b) and II(a); *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations* UNGA Res 42/22 (18 November 1987) annex para 8.

[363] Corfu Channel (n 148) 35; Nicaragua (n 96) 202.

[364] Nicaragua (n 96) 202ff; Philip Kunig, 'Intervention, Prohibition of' in MPEPIL (n 1) MN 1.

[365] Kunig (n 364) 3; Ulrich Beyerlin, 'Intervention' in Rüdiger Wolfrum and Christiane Philipp (ed), *United Nations: Law, Policies and Practice* (vol. I, CH Beck 1995) para 7; cf Georg Nolte ,'Article 2(7)' in Simma (n 223) MN 27; Katja S. Ziegler, 'Domaine Réservé' in MPEPIL (n 1) MN 1; d'Argent and Susani (n 258) 18.

[366] Kunig (n 364) 3; cf Fassbender (n 225) 70; Nolte (n 365) 27. Ziegler considers the impact of *domaine* réservé as 'more symbolic than legal', Ziegler (n 365) 32.

[367] Ziegler (n 365) 5.

In order to violate the non-intervention principle, 'coercion', as opposed to perfectly legal (political, economic, etc.) influence, must be employed.[368] The meaning of the term is unclear.[369] Scholars assert that illegal coercion implies massive influence, inducing the affected State to adopt a decision with regard to its policy or practice which it would not envision as a free and sovereign State.[370] The *Friendly Relations Declaration* (Principle 3) describes armed intervention, obtaining subordination of the exercise of a State's sovereign rights, and actions directed towards the violent overthrow of a regime of another State, as violating the non-intervention principle. This results in the notion that 'coercion' occurs only in drastic cases of overwhelming (direct or indirect) force being put upon a State's free and sovereign decision-making process.

Thus, it is not probable that, for example, the online law enforcement activities of foreign agencies (see para. 5.2.1.2.) would be considered by the affected State as meeting the threshold of impact as required by the notion of 'coercion'. The question of access to the internet or demands for the establishment of a national cyber security framework can surely not be deemed as violating the non-intervention principle, as such matters cannot be categorised as purely internal affairs of a State.

5.2.1.4. Duty Not To Harm Rights of Other States (Principle of Prevention, Precaution and 'Due Diligence')

Another principle aiming to de-conflict equal sovereignties of States is the duty not to harm the rights of other States and consequently, as confirmed by the ICJ,[371] not to let its own sovereign territory be used for activities causing damage to persons or objects protected by the sovereignty of another State (see also Article 1(2) of the UN Charter, endorsing a 'principle of equal rights').[372] The principle is closely related to the principle of good neighbourliness and the supporting maxim (or normative rule) *sic utere tuo ut alienum non laedas* (use your own property so as not to harm the one of another) is discussed *infra* in more detail.

The no-harm principle includes the obligation of States to take preventive measures in concrete cases of harm or risk of harm to other States' rights, of which the State in question has knowledge or presumptive knowledge.[373] Such an obligation can be derived from the logic of the no-harm obligation, and can be deemed as confirmed by the ICJ in the

[368] See discussion at Kunig (n 364) 5ff.

[369] ibid. The *Friendly Relations Declaration* also preserves a vague wording in this regard, see Keller (n 225) 20ff.

[370] Kunig (n 364) 22-27; Beyerlin (n 365) 809.

[371] Corfu Channel (n 148) 22.

[372] cf Heintschel von Heinegg (n 350) 7ff, 16 (with references).

[373] eg ibid; Epping and Gloria (n 295) § 26 MN 16.

Hostages[374] case (referring to preventive duties deriving from conventional and customary diplomatic law), and in the *Nuclear Weapons*[375] advisory opinion. It is endorsed in a multitude of treaties concerning the protection of the environment, nuclear accidents, space objects, international watercourses, management of hazardous waste and prevention of marine pollution.[376] An obligation to prevention is further enshrined in Article 3 of the ILC *draft Articles on Prevention of Transboundary Harm from Hazardous Activities*[377] of 2001, which states:

> 'The State […] shall take all appropriate measures to prevent significant transboundary harm [to the environment, persons or property] or at any event to minimize the risk thereof.'

According to the draft articles, such measures comprise, for example:

- risk assessment (Article 7),
- notification and information (Article 8), and
- consultation on preventive measures (Article 9).

These procedural duties are nowadays widely recognised as being part of international law, either in the form of international custom or of general principles of international law.[378] As Article 1 of the aforementioned draft indicates, these obligations might refer only to harm or risk of harm of physical nature. However, it could be argued that non-physical, though well perceptible, damage is relevant in the cyber context (para. 5.2.1.2.).

Furthermore, it can be attested that States are also obliged to take (general) precautionary measures with regard to potential cyber threats posing a significant risk of damage of a transboundary nature. The precautionary principle forms the basis of the legal regimes governing the high seas (*The United Nations Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks* of 1995) and Antarctica (*Protocol on Environmental Protection to the Antarctic Treaty* of 1991). Additionally, it is enshrined in several international treaties on

[374] Hostages (n 246) 68.

[375] Nuclear Weapons (n 103) 29.

[376] ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities,* with commentaries (2001) UN Doc A/56/10, General commentary, para 3 <http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf>; cf references at Philippe Sands, *Principles of International Environmental Law* (2nd edn, Cambridge University Press 2003) 246ff.

[377] See supra n 376.

[378] Handl (n 103) 541 (with further references).

environmental protection,[379] and is pronounced as either evolving[380] or already existing[381] customary rule of international environmental law.

As described above, it is certified by international courts and by scholarly writings that general principles of international law can, *inter alia,* be identified by deduction from the legal logic and from specific legal regimes or treaty regimes (see para. 5.1.1.). Once the existence of a general principle of international law is established in such a manner, and showing openness for concretisation in other circumstances, it can be applied to other situations or areas.[382] Such a technique does not present an analogy[383] (i.e., creation of new rules in cases of legal *lacuna*, by treating similar cases the same way legally)[384] in *sensu stricto*.[385] It should be mentioned that, due to the fact that the internet is another global resource beside the natural environment, and cyberspace is another common space beside the high seas and Antarctica, and that the area is sparsely regulated (see para. 5; especially the ITU rules on international telecommunications which do not entail cyber security regulations), an analogy would, in theory, seem not to be far-reaching. A common feature and overarching principle of the above-mentioned treaty regimes for globally shared resources and common spaces is the obligation to take precautionary measures, which is open for concretisation in other situations, and can subsequently be applied to the internet as another globally shared resource, and to cyberspace as another common space.[386]

Taking another conceptual approach, it was proposed in diplomatic circles (and is claimed by the US[387] to be an 'emerging norm') to introduce a principle of 'due diligence' of States (by a broad interpretation of the no-harm rule) with regard to malicious cyber activities of non-State actors originating from the States' territories and harming rights of other States. Given that all States acknowledge the relevance of malicious cyber activities for national and international peace and security, as shown by the multitude of respective UNGA resolutions,[388] including the establishment of all in all six GGEs (see para. 3.3.1.) on diverse cyber challenges, and by the adoption of Organisation for Economic Co-operation and

[379] cf discussion and references at Sands (n 376) 266-279.

[380] ibid 279; Winfried Lang, 'UN-Principles and International Environmental Law' (1999) 3 Max Planck Yearbook of United Nations Law 167.

[381] Ulrich Beyerlin and Jenny Grote Stoutenburg, 'Environment, International Protection' in MPEPIL (n 1) MN 24.

[382] Heintschel von Heinegg (n 124) § 19 MN 7.

[383] The use of a legal rule in an analogous way (*per analogiam*) means the application of a rule which covers a particular case to another case which is similar to the first but itself not regulated by the rule. See Silja Vöneky, 'Analogy in International Law' in MPEPIL (n 1) MN 1.

[384] ibid 4ff.

[385] Heintschel von Heinegg (n 124) § 19 MN 6ff.

[386] The application of principles of environmental law to the internet/cyberspace was first proposed by Torsten Stein and Thilo Marauhn, 'Völkerrechtliche Aspekte von Informationsoperationen' (2000) 60 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 21.

[387] The President of the United States of America (n 14) 10.

[388] See supra n 60-61.

Development (OECD) *Guidelines for the Security of Information Systems* [389] of 1992, it can be held that, assuming the thus confirmed common interest of States in cyber security, the duty to prevention could exceed concrete cases and be interpreted in general terms of a 'due diligence' (similar to the 'precautionary principle' as a general principle of international law applicable in to the internet and to cyberspace). Some scholarly writings assert that cyber security 'due diligence' is already part of international custom.[390]

The concrete features of preventive and precautionary (or the proposed 'due diligence') measures would stay within the discretion of the States.

However, the prevention principle obliges States to undertake a risk assessment and to inform, notify, and consult other States in concrete cases of harm and even of a significant risk of harm. This preconditions the ability of a State to notice irregular data streams or malicious software as such. This results, as a minimum, in the obligation of States to ensure that the national ISPs install network sensors collecting information on 'net flow', i.e., amount of routed data (allowing the detection of, e.g., 'DDoS attacks'), and that national tier 1 ISPs install intrusion detection/prevention systems at their 'gates' of international data transmission (see para. 3.5.), conduct deep package filtering (allowing recognition of malicious software), as well as a reporting system to a governmental entity (e.g., a national or governmental CERT). The conduct of the above described measures, the procedural obligations of notification, information and consultation, as well as the general management of the prevention of malicious cyber activities potentially harming other States' rights, requires the establishment of a framework of strategic, political, legal, administrative, organisational and technical nature. Additionally, the preventive principle would also oblige a State to establish investigative cyber capabilities (allowing the identification of the source of the malicious cyber activities) either within a CERT, the police or other security forces, depending on the division of responsibilities and authorisations pertaining to respective national laws (either existing or to be endorsed), as well as the organisational and legal framework allowing the prevention or discontinuation of concrete malicious cyber activities originating on the State's territory and potentially harming the rights of other States.

The precautionary principle (as well as the proposed 'due diligence' principle) includes the duty to undertake all appropriate regulatory and other measures at an early stage, and well before a harm or (concrete) risk of harm occurs.[391] This would involve the implementation of strategic, political, organisational, administrative, legal and technical measures (including the above-mentioned organisational, legal and technical measures) aimed at general prevention of the misuse of the possibilities that cyberspace offers for respective malicious activities by non-State actors, i.e., the establishment of a national cyber security framework. Such an obligation would apply only with regard to cyber activities possibly violating the rights of

[389] The guidelines call for cooperation of States (Principle 6) in the area of 'comprehensive protection' of information systems (Principle 4), and stipulate an imperative of deliberation in the use of information systems (Principle 3), OECD Doc OCDE/GD(92)190.

[390] Heintschel von Heinegg (n 350) 18.

[391] Sands (n 376) 246ff.

other States, thus inflicting severe damage (even if of a non-physical nature), i.e., with regard to cyber threats which can be deemed as clearly affecting other States' national security.[392] The specification of which malicious cyber activities would clearly affect the national security of States must be left to future State practice. It can be only assumed that, due to the interests of States, espionage activities would not fall under this category.[393] Nonetheless, the acknowledgement of the precautionary principle (or 'due diligence') for cyberspace entails the obligation to set up a national cyber security framework with regard to respective cyber threats (including these going beyond causing possible physical harm).

The recommendations on CBMs of the UN GGE (para. 3.3.1.) and, to a lesser extent, the draft CBMs of the OSCE (para. 3.3.2.) reflect the obligations to inform, notify, and consult in concrete cases of harm (information sharing on ICT incidents, exchanging of contact points for crisis management, including CERTs, cooperation to address security incidents). The existence of a national or governmental CERT, being an important aspect of a national cyber security framework, is hitherto presupposed (by referring to exchange of contact information of CERT personnel) by the UN GGE recommendations on CBMs (3.3.1.), and by the bilateral agreement between the US and Russia (para. 3.3.3.), and is proposed as a CBM only by the unilateral political declaration of Germany (para. 3.3.4.). The existence of a national cyber security framework can be seen as assumed by these sets of (draft) CBMs which refer to voluntary information sharing, e.g., about national organisations, programmes, or strategies relevant to ICT security (OSCE, para. 3.3.2.) or to an exchange of views and information about national strategies and policies, best practices, decision-making processes, relevant national organisations, and measures to improve international cooperation (UN GGE, para. 3.3.1.). The unilateral declaration of the Russian Federation, as reflected in the *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* of 2011, also presupposes the existence of a national cyber security framework, as it envisions the CBM of 'exchange of national concepts for ensuring security in the information space' (para. 3.3.4.).

It should be mentioned that, as stated above (para. 5.2.1.3.), demands for the establishment of a national cyber security framework (including the technical aspects thereof) cannot be deemed as a forbidden intervention in domestic affairs, as, due to the global nature of cyberspace and the internet, questions of cyber security do not fall under the category of purely internal matters.

5.2.1.5. Principle of Good Neighbourliness and sic utere tuo

Furthermore, balancing the competing sovereign rights of States, the principle of good neighbourliness has a relevance to cyberspace. The principle needs to be distinguished from the 'international law of neighbourliness' governing the relations of neighbouring States only

[392] Similarly: Heintschel von Heinegg (n 350) 16 (excluding cyber espionage and other 'mere intrusions into foreign computers or networks').

[393] ibid, though based on other deliberations.

in the frontier zones of their territories.[394] The principle of good neighbourliness is endorsed in a legally binding manner in the preamble of the UN Charter (where Article 74 refers to 'general principle of good-neighbourliness [...]' as a binding aim for policies with regard to colonies).[395] Moreover, the principle is endorsed as a legal obligation in international environmental law (especially referring to the use of trans-border resources such as rivers).[396] The principle mutually limits the sovereign exercise of activities potentially affecting neighbours in an intolerable manner, and is confirmed by the maxim (or normative rule) of *sic utere tuo ut alienum non laedas* (use your own property so as not to harm the one of another).[397] From the principle of good neighbourliness derive the obligations:[398]

- not to use or permit to use the territory in a manner as to cause damage to the territory of the neighbour State (see also para. 5.2.1.4.),
- to adopt any necessary – preventive and precautionary – measures in order to avoid or reduce damage beyond the own territory,
- to inform, notify, consult neighbours on any situation likely to cause damage beyond own territory,
- to tolerate activities otherwise not prohibited under international law so long as the consequences do not exceed an acceptable threshold of gravity (specified on a case-to-case basis).

As the principle of good neighbourliness had already been introduced to other types of vicinity than frontier regions (e.g., to contiguous and exclusive economic zones on the high seas or to 'regions'),[399] a further extension to cyberspace seems justified due to its global nature, to the speed and density of the internet connections and to its importance for inter-State relations of political, economic and other nature; aspects creating as a whole a modern form of 'vicinity'. This view can be deemed as confirmed by UNGA, which recognised already in 1991 that:

> 'great changes of political, economic and social nature, as well as the scientific and technological advances that have taken place in the word and led to unprecedented interdependence of nations, have given new dimensions to good-neighbourliness [...]',

[394] Laurence Boisson de Chazounes and Danio Campanelli, 'Neighbour States' in MPEPIL (n 1) MN 6-8.

[395] Ulrich Fastenrath, 'Article 74' in Simma (n 218) MN 2.

[396] ibid 2; cf Boisson de Chazounes and Campanelli (n 394) 18-20.

[397] Boisson de Chazounes and Campanelli (n 394) 10; Jutta Brunnée, 'Sic utere tuo ut alienum non laedas' in MPEPIL (n 1) MN 1, 15ff.

[398] Boisson de Chazounes and Campanelli (n 394) 11.

[399] ibid 12.

and emphasised that all States shall act as good neighbours 'whether or not they are contiguous'.[400]

However, the above-mentioned obligations deriving from the principle refer to physical damage only, a finding which can be considered as confirmed by Article 1 of the aforementioned ILC *Draft articles on Prevention of Transboundary Harm from Hazardous Activities*. As stated above, it could be suggested that the aspect of physical damage is irrelevant in the cyber context (para. 5.2.1.2.). Due to the enormous negative effects malicious cyber activities can have on the national security of another State it can be claimed that also harm of non-physical nature, though relevant to national security of another State, is governed by the principle of good neighbourliness.

This finding, comparable to the obligations deriving from the precautionary principle or from a potential 'due diligence' principle (see above), invokes the obligations of States to take preventive and precautionary measures (i.e., enhancing national cyber security) with regard to respective cyber threats, as well as obligations to inform, notify, and consult in cases of concrete risk or harm. Such features are partly reflected by the presented sets of (draft) CBMs for cyberspace (see deliberations at para. 5.2.1.4.).

5.2.2. Maintenance of International Peace and Security

Maintenance of international peace and security is the paramount purpose of the UN, enshrined in Article 1(1) of its Charter.[401] According to a systematic interpretation of the Charter, as well as according to the UNGA *Friendly Relations Declaration* and the *Proclamation of the International Year of Peace*[402] of 1985, peace is not understood negatively, as an absence of war or international armed conflict, but has become 'multidimensional',[403] requiring a series of active actions, taken collectively by States and peoples, *inter alia,* from the removal of various threats to peace and the development of CBMs (the latter also recommended by the UNGA *Friendly Relations Declaration*, Principle 1, para. 11).[404] The general principles of international law correlating to this aim are the duty to refrain from threat or use of force in international relations and the closely related duty to peaceful settlement of international disputes, both being the foremost means of prevention of war or international armed conflict.[405]

[400] UNGA Res 46/62 (9 December 1991) preamble, para 3 and operative part, para 2.

[401] d'Argent and Susani (n 258) 4.

[402] UNGA Res 40/3 (24 October 1985).

[403] d'Argent and Susani (n 258) 25.

[404] ibid 7; Rüdiger Wolfrum, 'Article 1' in Simma (n 223) MN 9ff.

[405] Albrecht Randelzhofer and Oliver Dörr, 'Article 2(4)' in Simma (n 223) MN 2.

5.2.2.1. Refrain from Threat or Use of Force in International Relations

The prohibition of threat or use of force in international relations constitutes one of the cornerstones of the international legal order.[406] The principle is endorsed in Article 2(4) of the UN Charter and is (in its core) widely considered as a peremptory norm of international custom.[407] According to the systematic, historical and teleological interpretation of the UN Charter, as well as by the jurisprudence of the ICJ and by scholarly writings the term 'force' is to be understood as 'armed force'.[408] The term 'use of [armed] force', however, is not limited to the employment of military weaponry in the common sense of the term.[409] The ICJ attested over 25 years ago in its *Nicaragua*[410] case the possibility of an 'indirect' or non-military use of armed force (e.g., by arming and training insurgents) and scholarly writings describe, for example, spreading fire over the border or flooding another State's territory as violating the prohibition of 'use of [armed] force'.[411]

In order to specify the meaning of 'use of [armed] force' conducted by means of the internet or other ICTs, an effects-based approach inherent to public international law is appropriate (ruling out other possible approaches, e.g., focusing the target of the malicious activities, the intent of the malevolent actor, or the categorisation of the means used).[412] Hereby, a comparison of the effects indirectly caused or intended by malicious cyber activities with the effects usually caused or intended by conventional, biological or chemical weapons (BC weapons) is necessary.[413] According to the traditional understanding, 'use of [armed] force' requires the employment of kinetic weaponry, i.e., of a tool designed to cause kinetic effects of a physical nature on a body or on an object. The transfer of data and its delay or interruption, as well as the manipulation, suppression or deletion of data cannot be deemed to cause (directly) kinetic effects in the common meaning of the term. In contrast, some similarities between malicious cyber activities and BC weapons can be conceived. The use of BC weapons does not cause destruction in conventional sense, as these weapons do not set free kinetic energy.[414] The employment of BC weapons is considered as a form of 'use of

[406] ibid 1; Oliver Dörr, 'Use of Force, Prohibition of' in MPEPIL (n 1) 1; cf Nicaragua (n 96) 190 ('fundamental or cardinal principle of […] [customary international] law').

[407] Randelzhofer and Dörr (n 405) 64-68; Dörr (n 406) 1, 10, 32; Wolfrum (n 158) 45; d'Argent and Susani (n 258) 23; Ziolkowski (n 333) 200-205 (with further references); Nicaragua (n 96) 100. See scepticism due to contrary State practice at Michael J. Glennon, *Limits of Law, Prerogatives of Power: Interventionism after Kosovo* (Basingstoke 2001) 44, 56 and idem, 'Why the Security Council Failed' (2003) 82 Foreign Affairs (3) 23ff.

[408] cf Dörr (n 406) 11; Marco Roscini, 'World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force' (2010) 14 Max Planck Yearbook of United Nations Law 104-106; see also Randelzhofer and Dörr (n 405) MN 16-20; Thomas Bruha, 'Use of Force, Prohibition of' in Wolfrum and Philipp (n 365) 1387ff.

[409] Randelzhofer and Dörr (n 405) 21; Dörr (n 406) 12 (referring explicitly to cyber means).

[410] Nicaragua (n 96) 228.

[411] Randelzhofer and Dörr (n 405) 21; Dörr (n 406) 12.

[412] Similar Randelzhofer and Dörr (n 405) 22.

[413] cf Randelzhofer and Nolte (n 329) 43.

[414] Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 New York University Journal of International Law and Politics 72; Todd A. Morth, 'Considering Our Position: Viewing

[armed] force' because they can cause death or injury to living things.[415] Thus, in the case of BC weapons, the term 'weapon' is defined with reference to their effects rather than their method, which perfectly corresponds with the effects-based approach inherent to public international law. Consequently, the majority of scholars rightly insist on an effects-based interpretation of the term of 'use of [armed] force' in the cyber context.[416] Therefore, it can be assumed that malicious cyber activities can be considered 'use of [armed] force' in the meaning of Article 2(4) of the UN Charter if they – indirectly – result in:[417]

- deaths or physical injuries of living beings and/or the destruction of property.[418]
- massive, medium to long-term disruption of critical infrastructure systems of a State (if in its effects equal to the physical destruction of the respective systems).[419]

In contrast, neither the mere destruction of data (even of substantial importance, e.g., classified data, or of significant economic value, e.g., symbolising assets)[420] nor the 'theft'[421] (rather, illegal copying) of data (being nothing more than modern espionage[422] neither

---

Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 Case Western Reserve Journal of International Law 590.

[415] Brownlie (n 91) 362.

[416] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law (3) 913 and 919; Stein and Marauhn (n 386) 6.

[417] For detailed discussion see Katharina Ziolkowski, 'Computer Network Operations and the Law of Armed Conflict' (2010) 49 Military Law and the Law of War Review 69-75.

[418] Randelzhofer and Nolte (n 329) 43; Yoram Dinstein, 'Computer Network Attack and Self-Defense' in Michael N Schmitt and Brian T O'Donnell (eds), *Computer Network Attack and International Law* (US Naval War College 2002) 103; Daniel B. Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' in Schmitt and O'Donnell (supra) 85; Barkham (n 414) 80; Stein and Marauhn (n 386) 7; Joyner and Lotrionte (n 353) 846 and 850; Walter G. Sharp, *Cyberspace and the Use of Force* (Aegis Research Cooperation 1999) 102; Schmitt (n 416) 914ff; Morth (n 414) 591; Greenberg, Goodman and Soo Hoo (n 353) 19 and 32.

[419] Randelzhofer and Nolte (n 329) 43; Ziolkowski (n 417) 69-75; James P Terry, 'Responding to Attacks on Critical Computer Infrastructure. What Targets? What Rules of Engagement?' in Schmitt and O'Donnell (n 418) 428ff; Morth (n 414) 599; Sharp (n 418) 129ff. Contra: Michael N Schmitt, 'The 'Use of Force', in 'Cyberspace: A Reply to Dr Ziolkowski' in Czosseck, Ottis, Ziolkowski (n 12) 315; Dinstein (n 418) 105; Stein and Marauhn (n 386) 8, who demand the occurrence of physical damage outside the targeted computer networks in order to qualify CNO as use of force.

[420] cf Michael N Schmitt, Heather A Harrison Dinniss and Thomas C Wingfield, *Computers and War: The Legal Battlespace* (International Humanitarian Law Research Institute, Background Paper 2004) 5ff; Barkham (n 414) 88.

[421] Joyner and Lotrionte (n 353) 846, 855ff; contra: Stein and Marauhn (386) 10.

[422] Anthony D'Amato, 'International Law, Cybernetics, and Cyberspace' in Schmitt and O'Donnell (n 418) 67; Stein and Marauhn (n 386) 32 (with further references). With regard to cyber activities as modern form of espionage, cf Wolff Heintschel von Heinegg, 'Informationskrieg und Völkerrecht. Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung' in Volker Epping, Horst Fischer and Wolff Heintschel von Heinegg (eds), *Brücken bauen und begehen. Festschrift für Knut Ipsen zum 65. Geburtstag* (CH Beck 2000) 134. Apart from the penalisation of espionage resulting from respective national law systems, spying is restrained by certain provisions of public international law, eg, the taboos stated by the diplomatic and consular law protecting diplomatic and consular archives and correspondence, i.e., respective electronic databases and communication via the internet.

generally permitted nor forbidden under public international law) can be considered 'use of [armed] force'.[423] Such effects cannot be equated to the effects usually caused or intended by conventional or BC weapons, especially not to the physical destruction of objects.[424]

'Use of [armed] force' in the meaning of Article 2(4) of the UN Charter is to be distinguished especially from measures of mere (economic or political) coercion in international relations, a task that can pose considerable challenges upon decision-makers in practice. For facilitating such a distinction, in 1999[425] Professor Schmitt developed and recently reinforced[426] a set of criteria for the determination of 'use of [armed] force' (amending their descriptions over time), namely severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy (or legality) and responsibility.[427] The factors shall serve as indicators which States are likely to take into consideration when assessing whether specific malicious cyber-activities qualify as 'use of [armed] force'.[428] However, they are not meant as legal criteria.[429]

State practice and *opinio iuris,* apart from a vague political declaration of the US[430] to respond to 'hostile acts in cyberspace' with self-defence measures, is hitherto not detectable.

As mentioned above (para. 5.2.1.1.), the sets of (draft) CBMs do not reflect the duty to restrain the use of force in international relations. Although States in general prefer to maintain a strategic ambiguity with regard to questions related to use of force, thus leaving the debate to academia, it would certainly support predictability and thus stability in international relations, if they shared their views in this aspect.

5.2.2.2. Peaceful Settlement of Disputes

The legal[431] obligation to peaceful settlement of international disputes is endorsed in Article 2(3) of the UN Charter, specified by the UNGA in its *Friendly Relations Declaration* as well as

[423] Ziolkowski (417) 69-75.

[424] cf ibid for detailed discussion.

[425] Schmitt (n 416) 913ff.

[426] idem (n 333) 576ff (the criterion of 'responsibility' was mentioned already in the 1999 publication, although only in a footnote, see idem (n 416) 915, footnote 81).

[427] ibid 576ff.

[428] ibid 605.

[429] Schmitt (n 419) 314; see also discussion of the criteria: Katharina Ziolkowski, '*Ius ad bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force' in Czosseck, Ottis, and Ziolkowski (n 12), 295-309.

[430] The President of the United States of America (n 14) 12ff.

[431] cf Christian Tomuschat, 'Article 2(3)' in Simma (n 223) MN 23; Wolfrum (n 158) 44.

in the *Manila Declaration on the Peaceful Settlement of International Disputes*[432] of 1982, and recognised by the ICJ as a 'principle of customary international law.'[433]

The principle limits the notion of sovereignty and correlates to the principle of the restraint of threat or use of force in international relations, recognising that unsettled disputes can lead to eruptive disturbances within the international community.[434] The dispute in question does not need to endanger international peace and security (see on the other hand Article 33-38 of the UN Charter). The pacific means of dispute resolution consist of diplomatic-political measures (e.g. negotiation, inquiry, mediation, conciliation) and legal measures (arbitration and litigation) (compare Article 33(1) of the UN Charter).[435] Although no compulsory instrument of adjudication exists, the majority of scholars deem the principle as establishing an obligation to deploy active efforts to settle international disputes (in the meaning of conduct, not outcome).[436] With regard to the means of peaceful settlement of international disputes, States have a wide-ranging discretion, although the UN Charter contains some proposals in Chapter VI concerning disputes endangering international peace and security (including investigative powers of the UNSC and the possibility to bring a dispute to the attention of UNGA or UNSC).[437]

A violation of the principle can only be affirmed if a party to an international dispute constantly refuses to even attempt to reach a settlement.[438] Thus, in cases of a concrete international dispute with regard to the cyber realm, on whichever aspect and of whatever intensity or possible consequences, the respective States have a legal obligation to attempt to seek a peaceful solution, but nothing more. In this sense, the obligation of peaceful settlement of disputes is a variation of the duty to cooperation. Additionally, if the dispute evolved on the grounds of unlawful behaviour of a State, the State(s) affected could have the possibility to recourse to retorsions (unfriendly acts) or counter-measures (para. 3.4.1.).

5.2.3. Cooperation and Solidarity

The general duty of cooperation is to be distinguished from the 'law of coexistence' and from the political concept of 'peaceful co-existence'. The former is a legal principle deriving from the beginnings of modern international law (strongly focusing sovereignty of States), which forms the basis of the contemporary duty to cooperation.[439] The latter is a political

[432] UNGA Res 37/10 (15 November 1982).

[433] Nicaragua (n 96) 290.

[434] Tomuschat (n 431) 2; d'Argent and Susani (n 258) 13.

[435] Anne Peters, 'International Dispute Settlement: A Network of Cooperational Duties' (2003) 14 European Journal of International Law (1) 4.

[436] Tomuschat (n 431) 24ff; contra: Peters (n 435) 9.

[437] Tomuschat ibid.

[438] ibid 25.

[439] Rüdiger Wolfrum, 'Co-operation, International Law of' in MPEPIL (n 1) MN 1; cf Fassbender (n 225) 3-14.

doctrine, pursued by the Soviet Union and, with some differences, also by the Chinese foreign policy until the end of the Cold War (still endorsed in the *Constitution of the People's Republic of China*).[440]

The duty of States to cooperation has a normative character whenever it is endorsed in international treaties establishing and governing international organisations.[441] The existence of a *general* duty to cooperate and its legal character is disputed among scholars.[442] However, there are convincing indications for the normative character of a *general* duty to cooperate, when considering the interdependence of States in times of globalisation, the enormous number of intergovernmental organisations (approximately 7,000), the myriad of international treaty obligations governing almost all aspects of international relations (over 50,000 are registered at the UN), and the endorsement of the duty of cooperation in the almost universal UN Charter. This finding is supported by the emergence of an intensified form of cooperation through 'transgovernmental networks', i.e., direct interaction of specialised domestic officials in informal or formal modes, which is conditioned by the 'information age' and augmenting the traditional inter-State cooperation.[443]

The UN Charter sets as one of the purposes of the organisation (and indirectly as an obligation of its member States) 'to take effective collective measures' to maintain international peace and security (Article 1(1)) and '[t]o achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character [...]'(Article 1(3)). The *Friendly Relations Declaration* emphasises the development of cooperation among States as 'of the greatest importance for the maintenance of international peace and security' (preamble, para. 5). Principle 4 of the declaration (*The duty of States to co-operate with one another in accordance with the Charter*) states:

> '[…] States shall co-operate with other States in the maintenance of international peace and security […]. States shall conduct their international relations in the economic, social, cultural, technical and trade fields […]. States should co-operate […] in the field of science and technology […].'

[440] Carlo Panara, 'Peaceful Coexistence' in MPEPIL (n 1) MN 1ff and 29. The doctrine focuses the importance of a peaceful cohabitation, including even forms of cooperation, between 'imperialist' and socialist States that would though be not equivalent with 'peace'. See ibid 38.

[441] ibid 5.

[442] See for arguments pro and con: Wolfrum (n 439) 13-24; Jost Delbrück, 'The International Obligation to Cooperate – An Empty Shell or a Hard Law Principle of International Law? – A Critical Look at a Much Debated Paradigm of Modern International Law' in Holger P Hestermeyer et al. (eds), *Coexistence, Cooperation and Solidarity. Liber Amicorum Rüdiger Wolfrum* (vol 1, Brill 2011) 3-16.

[443] Kal Raustiala, 'The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law' (2002) 43 Virginia Journal of International Law (1) 3ff and 10ff.

Thus, given the universality of the UN and the importance of the declaration (para. 5.1.1.), nearly all States have a conventional obligation to cooperate, also in the realm of cyberspace, as far as it supports the maintenance of international peace and security.

Furthermore, a legal obligation of States to cooperate in the arena of cyber security can be derived from the global character of cyberspace. A legal obligation to cooperate was created by international treaties governing common spaces, as in Articles II and III of *The Antarctic Treaty* of 1959, Articles III and IX-XI of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* of 1967, and Part XI of the *United Nations Convention on the Law of the Sea* of 1982. Furthermore, the obligation to cooperate is endorsed in the myriad of international agreements governing environmental protection.[444] As described in more detail above (para. 5.2.1.4.), general principles of international law can, *inter alia,* be identified by deduction from specific legal regimes or treaty regimes (these governing globally shared resources and common spaces) and applied to the internet as another globally shared resource and to cyberspace as another common space.

The term 'cooperation' is not defined by an international treaty or in another multilateral document. However, based on an analysis of the *Friendly Relations Declaration*, cooperation can be perceived as the voluntary and proactive joint action of two or more States which serves a specific objective.[445] Consequently, the duty to cooperate can be described as 'the obligation to enter into such co-ordinated action as to achieve a specific goal',[446] which can be effectively undertaken by the States working together or when the interests of the international community require a joint action.[447]

Although the notion of 'cooperation' remains vague, the concept of solidarity indicates that cooperation in the cyber realm should show a heightened intensity. The concept of solidarity, to which some scholars[448] attribute emerging normativity (because of references in UNGA Resolutions and endorsement as a legal obligation in several international treaties),[449] supports the interpretation of international law.[450] Solidarity can be understood as an intensified form of cooperation for fostering common interests and shared values.[451]

[444] Wolfrum (n 439) 31.

[445] ibid 2; Peters (n 435) 2.

[446] ibid; Wolfrum (n 439) 31.

[447] ibid.

[448] Abdul G. Koroma, 'Solidarity: Evidence of an Emerging International Legal Principle' in Hestermeyer (n 442) 103-130; R. St John McDonald, 'Solidarity in the Practice and Discourse of Public International Law' in (1996) 8 Pace International Law Review 301; Holger P Hestermeyer, 'Reality or Aspiration? – Solidarity in International Environmental and World Trade Law' in ibid (n 442) 48ff.

[449] eg Article 3(b) of the *United Nations Convention to Combat Desertification in Those Countries Experiencing Serious Drought and/or Desertification, Particularly in Africa* of 17 June 1994, Article 3(a) of *The Constitutive Act of the African Union* of 11 July 2000 (before: Article II(1)(a) of the OAU Charter of 25 May 1963); UN *Millennium Declaration* (n 217) para 6; for further references see Hestermeyer (n 448) 50.

[450] Danio Campanelli, 'Solidarity, Principle of' in MPEPIL (n 1) MN 21; Hestermeyer (n 442) 48ff.

[451] Wolfrum (n 439) 3.

Especially, the concept is underlying, *inter alia,* the legal regimes governing the globally shared resource of natural environment and the common space of the sea bed.[452] The recognition of the concept of solidarity for the arena of the internet and cyberspace is justified on the grounds that the internet presents another global resource and cyberspace another common space, which certainly is in the common interest of the international community. Additionally, it seems reasonable that an intensified interdependence in the field of global communications (leading to an international community united in solidarity)[453] would result in the need for an intensified cooperation.

Due to the global nature of the internet and cyberspace, the integrity of these 'ecosystems' and the reduction of cyber threats as relevant to national and international security can be deemed as of common interest of the international community and can only be effectively conducted by the joint efforts of all States. Therefore, States have a legal obligation to cooperate in this regard. Additionally, based on the notion of the internet as global resource and of cyberspace as common space, the cooperation should show a 'heightened' intensity. However, States have a wide discretion as to how to fulfil the legal obligation to cooperate in the cyber realm.

The cooperation measures as envisioned by the UN GGE in the recommendations on CBMs for cyberspace (para. 3.3.1.) and as currently negotiated within OSCE (para. 3.3.2.) indicate a concretisation of the general legal obligation to cooperate. It is, however, doubtful whether these (draft) measures meet the requirement of the intensity as necessitated by the interdependence and subsequent solidarity of the international community in the cyber arena.

5.3. Some Thoughts de lege ferenda for Cyberspace

In terms of *lex ferenda*, some basic general principles of international law, as deduced from the legal regimes governing the protection of the international environment, of common spaces (sea bed, outer space, Antarctica), or the protection from globally spreading (health) infections, could be identified and applied to the internet as a globally shared resource or to cyberspace as a common space (see para. 5.2.1.4. on the juridical technique). The following deliberations *de lege ferenda* will consider, however, only the very basic principles underlying the specific regimes, as postulating utopian ideas as general principles of international law would certainly harm[454] the normativity of law.

It should be mentioned that all principles as subsequently described can also be indirectly deduced from the principles of equal sovereignty of States and the duty of cooperation. Additionally, it can be asserted that the *de lege ferenda* application of the principle of

[452] Campanelli (n 450) 6; McDonald (n 448) 262 and 282-290.

[453] cf Ahmed Mahiou, 'Interdependence' in MPEPIL (n 1) MN 17.

[454] cf von Bogdandy (n 160) 1913.

sustainable development and equitable utilisation of global resources (5.3.1.), of common heritage or concern of humankind (5.3.2.), and of the protection against globally spreading (health) infections (5.3.3.) to cyberspace or to the internet would certainly support the legal obligation of States to the maintenance of international peace and security and, in a broader sense, of removal of various threats to peace and security.

5.3.1. Sustainable Development and Equitable Utilisation of Shared Resources

The principle of sustainable development was first mentioned within the UN in the 1970s, pointing out the linkage of long-term development (in particular, of the so-called 'Third World') and environmental protection and has, since then, been referred to in a multitude of legal and political documents.[455] The concept is based on the notion that development which meets the needs of the present generation shall not compromise the abilities of future generations, and that the use of natural resources shall be conducted in accordance with ecological, economic and social considerations.[456] It is disputed whether sustainable development is a political ideal or whether it can be deemed as a rule of international customary law.[457] One of the sub-categories of the concept, the rule of sustainable use (with regard to natural resources), is, however, widely attested to have the character of a norm of international customary law, due to its endorsement in a large number of international environmental protection agreements.[458] Additionally, the principle of equitable utilisation of shared resources (developed in the context of international water resources and the continental shelf) is acknowledged as a general principle of international law, and is endorsed in various international agreements, UNGA resolutions and political declarations, and is confirmed by the international jurisprudence.[459] Therefore, the rule of sustainable and equitable use of resources can be deemed a general principle of international environmental law, and can be applied (para. 5.2.1.4.) to internet as another globally shared resource, establishing a legal obligation of States to cooperate in sustainable and equitable usage.[460] This assumed, the principle shows relevance to the internet in a twofold manner:

(1) At the first sight, the internet could be seen as not exploitable in terms of usage. This is not true, as the internet is conditioned by the possibility of individual connectivity to the web, which requires an IP address (see note 89). The Internet Protocol version 4 (IPv4) currently used in most parts of the globe provides only approximately four billion IP addresses, which was deemed sufficient in the pioneer days of the internet

[455] cf Ulrich Beyerlin, 'Sustainable Development' in MPEIL (n 1) MN 1ff.

[456] ibid 1; Wolfrum (n 158) 50.

[457] cf Beyerlin (n 455) 15ff (with further references).

[458] ibid 20; Lilian del Castillio-Laborde, 'Equitable Utilisation of Shared Resources' in MPEPIL (n 1) MN 2-6 (with further references); Sands (n 376) 252ff, 257ff (with further references).

[459] cf del Castillio-Laborde (n 458) 8ff (with further references) and 27. See also *Report of the Expert Group Meeting on Identification of Principles of International Law for Sustainable Development* (Geneva, Switzerland, 26-28 September 1995, Prepared by the Division for Sustainable Development for the UN Commission on Sustainable Development) para 38 and paras 48-50.

[460] On obligations cf del Castillio-Laborde (n 458) 15, 25.

but have been officially exhausted since February 2011.[461] Nowadays, the Internet Protocol version 6 (IPv6) can provide approximately 340 sextillion IP addresses, which is presently considered as more than sufficient for the world population of about seven billion (enough for many trillions of IP addresses to be assigned to every human being).[462] However, IPv6 is not compatible with IPv4 and is implemented only in some parts of the world.[463] This means that, despite the technological advance, IPv6 communication needs very often to be 'channelled' through the existing and limited IPv4 communication lines. Once implemented globally, IPv6 will, *de facto,* eliminate the notion of 'exploitation' of the global resource and mitigate the challenge of equitable distribution of access to, and thus use of, the internet. However, the IPv6 address range, although extremely large, it is not indefinite. Future developments can prove the number of IP addresses as not 'enough for everybody', e.g., when considering the enormous need for IP addresses by future manufacturing by 'smart factories', combining globally distributed production processes via wireless local area networks (WLANs) and thus requiring masses of IP addresses. In this context, a 'lesson identified' from the past should not be ignored: Bill Gates is said to have stated in 1981 that '640K ought to be enough for anybody',[464] a prediction undeniably proven wrong even with regard to the private use of computers. Therefore, the 'exploitation of the internet' is, in theory, conceivable. The consequence of this presupposition is a reasonable, equitable use of IP addresses in terms of an internationalised, just and fair regime for their worldwide distribution (conducted at the present by ICANN[465]).

(2) The legal obligation of 'sustainable use' of the internet, recognising the needs and interests of future generations, could also result in an obligation of States to undertake all necessary means of a strategic, political, legal, administrative, organisational and technical nature at an international (cooperatively) and national (individually) level in order to preserve the internet (and thus also cyberspace) for future generations as an available and reliable platform of political, economic, social and cultural interaction for all users. This connotes the restraint from any governmental action which could hamper the availability and reliability of the internet, and the proactive countering of cyber threats; even those irrelevant to national and international security.

---

[461] Internet Society, IPv6 <http://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6>. IANA, Number Resources <http://www.iana.org/numbers>.

[462] ibid. For explanation of the numbers of IP addresses see <http://www.brucebnews.com/2010/10/ipv6-and-really-large-numbers/>.

[463] cf Internet Society, IPv6 (n 461).

[464] <http://en.wikiquote.org/wiki/Talk:Bill_Gates>.

[465] See supra n 327. Since February 2005, ICANN delegates the assignment of IP addresses to individual users of IP address ranges to ISPs to five *Regional Internet Registries* (RIR), i.e., regional organisations assigning IP addresses. Currently, these are: AfriNIC (Africa), APNIC (Asia and Pacific), ARIN (mainly North America), LACNIC (Latin America and parts of the Caribbean Region) and RIPE NCC (Europe, Middle East and Central Asia). The RIRs assign the IP addresses to local organisations, mainly to ISPs (eg, yahoo, gmail, etc.). Usually, an internet user receives from the pool of IP addresses at the disposal of an ISP a specific (dynamic) IP address for the particular internet session only. After the particular internet session the dynamic IP address is assigned to another user and client of the respective ISP.

At the moment, only the set of CBMs as recommended by the UN GGE exceeds the traditional notion of CBMs as a tool of prevention of the outbreak of a war or international armed conflict by misunderstanding or misperception, and seems aimed at enhancing overall cyber security (para. 3.3.1.), which corresponds to the principle of sustainable development of the global resource internet.

5.3.2. Common Heritage or Concern of Humankind

The principle of common heritage of humankind is underlying and governing the treaty-based regimes of certain common spaces (*res communis omnium*), namely:

- the seabed (Part XI of the UN *Convention on the Law of the Sea* of 1982),
- outer space (Article 1 of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* of 1967, Article 11(1) of the *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* of 1979), and
- Antarctica (para. 8 of the preamble of the *Protocol on Environmental Protection to the Antarctic Treaty* of 1991).

Although the application of the principle varies in the different legal regimes, and is probably not intended to be fully defined, some common features can be identified, such as:[466]

- exclusion of claims of sovereignty (non-appropriation; open to use by all),
- international management (by the mankind as a whole),
- obligation to:
    - international cooperation in use and exploration (regulated, equal distribution to benefit of all humankind with regard to utilisation and exploration),
    - respect for interests of future generations in making use,
    - usage for peaceful purposes only.

The principle of common heritage of humankind is also applied to other common spaces than the above-mentioned, namely to the high seas, the atmosphere, and to the natural environment as such (using the term of common 'concern' of humankind with regard to the latter).[467] It is also asserted that the principle could be applied outside of common spaces,

[466] Rüdiger Wolfrum, 'Common Heritage of Mankind' in MPEPIL (n 1) MN 11-24.

[467] ibid 9; Crawford (n 132) 333.

namely to living resources.[468] Thus, although the principle of common heritage (or concern) of humankind was not meant to constitute an independent principle, its application outside the respective, above-mentioned treaty regimes, i.e., to cyberspace, seems to be, in theory, adequate. This is supported by the assertion that the principle obtained the character of international customary law with regard to the use of common spaces (resulting in obligations to international cooperation, use for peaceful purposes, equal distribution of usage and exploration, and respect for future generations).[469]

Although cyberspace can surely be deemed a common space or 'global common' in general terms, it is questionable whether it has developed[470] to a *res communis omnium* in the legal sense. Cyberspace, understood as a universal, non-physical, conceptual space, including, *inter alia,* information and a 'global public memory' (see definition in para. 1) involves the notion of the internet. The physical and technical components of cyberspace, i.e., the internet, are subject to territorial sovereignty of diverse States, although forming in its assemblage a global resource. Thus, only within the notion of the internet as a whole, i.e., as a global resource, the exclusion of claims of sovereignty (or appropriation) can be affirmed and the principle of common heritage or concern of humankind could be applied to cyberspace.[471] However, the global internet, although managed mainly by the (privately-owned or governmental) ISPs, can be deemed as 'governed' by ICANN (based on a multitude of agreements with a myriad of stakeholders), an NGO of an internationalised character, however, acting on behalf of and reporting to the US government (see above, para. 5.2.1.). Therefore, it can be either accepted or doubted whether the aspect of an 'international management' of the internet is given.

If the internet, and thus cyberspace, was considered a common heritage or concern of humankind, States would have the obligation to, *inter alia,* use it for peaceful purposes only. This corresponds with the general principle of international law to restrain from the threat of or the use of force in international relations, and would still allow the military use of cyberspace for, e.g., exercises, self-defence, or measures undertaken according to Chapter VI and VII of the UN Charter. Although States partly refer to cyberspace as a 'global common',[472] the official diplomatic language partly avoids terminology which could indicate the development of cyberspace into a common heritage or concern of humankind (e.g., Germany speaks of a 'public good'[473]). Thus, tendencies for respective developments are momentarily not detectable.

---

[468] Wolfrum (n 158) 61.

[469] idem (n 466) 25.

[470] Affirming cyberspace as *res communis omnium*: Heintschel von Heinegg (n 350) 9.

[471] ibid.

[472] eg Japan, Ministry of Defence (n 5) 2; US Department of Defence, *The Strategy for Homeland Defence and Civil Support* (2005) 12.

[473] Permanent Mission of the Federal Republic of Germany to the United Nations, New York, Note Verbale/Note No 516/2012 (November 2012) <http://www.un.org/disarmament/topics/informationsecurity/docs/Germany_Verbal_Note_516_UNODA.pdf>.

5.3.3. Protection against Globally Spreading Infections – The World Health Regime

International cooperation in the field of transboundary spreading of health infections had already begun in the 19th century.[474] It was motivated by technological advances of communication and transportation, which led to intensified economic exchanges and international relations.[475] The World Health Organization (WHO), established in 1948, is providing leadership on global health matters, setting norms and standards, articulating evidence-based policy options, providing technical support to countries as well as monitoring and assessing health trends.[476] According to Article 21 of the WHO Constitution, the Health Assembly (pursuant to Article 10 composed of delegates representing all member States) has the authority to adopt regulations on:

(a) quarantine requirements and other procedures designed to prevent the international spread of disease,

(b) nomenclatures with respect to diseases,

(c) standards on safety and other areas,

(d) standards on purity of products moving in international commerce, and

(e) advertising and labelling of products moving in international commerce.

According to Article 22 of the WHO Constitution, the regulations come into force by use of a silent-procedure. Such International Health Regulations (IHR) entered into force in 2007, and are legally binding on 194 countries across the globe, including all the member States of the WHO.[477] They define, *inter alia,* the obligations of States to report public health events and require States to strengthen their existing capacities for public health surveillance and response.[478] Furthermore, pursuant to Article 28(i) of the WHO Constitution, the WHO Board (consisting of 34 persons designated by the Health Assembly, Article 24) has the authority 'to take emergency measures […] to deal with events requiring immediate action.'

Based on the truly universal normativity of the IHR, a general principle of international law in the form of an obligation of intense cooperation between States for the prevention and combat of infections (or diseases) can be derived from that legal regime (including obligations to inform, notify, and consult). However, the application (see para. 5.2.1.4. for the legal technique) of the principles underlying the IHR to the situation of transboundary spreading of computer viruses, worms and other malicious software does not seem justified, as the impact of malicious software on world populations is very different in its intensity and significance from the impact of globally spreading health infections and diseases. The

[474] Yves Beigbeder, 'World Health Organization (WHO)' in MPEPIL (n 1) MN 2.

[475] ibid.

[476] WHO, About WHO <http://www.who.int/about/en/>.

[477] idem, 'What are the International Health Regulations?' <http://www.who.int/features/qa/39/en/index.html>.

[478] ibid.

massive negative impact of cyber manipulations on economies, which cannot be denied, does not vindicate the application of the principles of health regulations to the internet or to cyberspace.

However, empowering an international entity with authorities comparable to those which the WHO Health Assembly and Board have (see above) should be considered. As the impact of cyber threats on national and international security will surely intensify in future due to technological advances and a growing dependence on the global net, such an international entity could adopt regulations regarding:

- reporting of cyber security incidents,
- quarantine requirements for networks,
- nomenclatures of malicious software,
- standards of cyber security,
- standards of purity of software,
- advertising and labelling of software, and
- taking emergency measures in cases which require immediate action.

6. Implications for NATO

NATO is a collective defence alliance of the nature of a politico-military international organisation. Emerging in the post-World War II era as a collective security mechanism, since the end of the Cold War, the Alliance has displayed a transition into an organisation with comprehensive definitions of security threats and an almost global outreach through its partnership programmes. These developments are perfectly consistent with the broad mandate of NATO, as endorsed in Article 2 of the North Atlantic Treaty of 1949. The provision obliges the member States to 'contribute toward the further development of peaceful and friendly international relations' by, *inter alia*, 'promoting conditions of stability'.

Accordingly, NATO member States recognised in the *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation* of 2010 that malicious cyber activities 'can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability'.[479] The current NATO *Policy on Cyber Defence* of 2011 focuses NATO on the protection of its own communication and information systems in order to perform

[479] NATO, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation* (adopted by Heads of State and Government at NATO, 19-20 November 2010, Lisbon) para 12 <http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf>.

the Alliance's core tasks of collective defence and crisis management.[480] However, as cyber threats transcend State borders and organisational boundaries, the policy also stresses the need for cooperation of the Alliance with NATO partner countries.[481] NATO member States reinforced the importance of international cooperation by stating in the *Chicago Summit Declaration* of 2012 that:

> '[t]o address the cyber security threats and to improve our common security, we are committed to engage with relevant partner countries on a case-by-case basis […] in order to increase concrete cooperation.'[482]

NATO surely cannot be a platform for negotiations of CBMs for cyberspace among its member States, as Allies by nature do not need to build confidence in order to reduce the risk of an outbreak of an (international) armed conflict among them. However, NATO is preconditioned to being a group of 'like-minded' States, sharing common values and showing good prospects of unifying efforts in the international peace and security arena by using cyber defence fora at the political, organisational and tactical levels, as the organisation currently disposes of, for discussions. Such unified efforts with regard to negotiations of CBMs for cyberspace could be currently hampered by the diversity of the member States with regard to the development of cyber infrastructure, national cyber security frameworks, and the role cyberspace plays for administration, industry and civil society. However, commitments on CBMs for cyberspace between NATO member States and partner nations are certainly of interest to the organisation, as CBMs aim to strengthen international peace and security in the context of cyber security. Thus, the respective endeavours of NATO's member States definitely correlate to the purpose and spirit of the organisation's mandate and NATO's recognition of malicious cyber activities as a potential threat to the security of the Alliance.

The development of a joint position of NATO member States on CBMs for cyberspace or conducting an in-depth study about the applicability of CBMs to cyberspace, as mentioned above (para. 3.2.), within NATO's *Science for Peace and Security Programme* would certainly support the work of the international community as presented above (para. 3.3.). However, even if not actively supporting the negotiations of CBMs for cyberspace, it could be beneficial for the organisation to closely observe respective developments, especially as occurring in the fora of other international organisations, e.g., by the delegation of observers.

---

[480] idem, Public Diplomacy Division, 'Defending the networks. The NATO Policy on Cyber Defence', Factsheet <http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf>.

[481] idem, 'NATO and cyber defence', website <http://www.nato.int/cps/en/SID-714ABCE0-30D8F09C/natolive/topics_78170.htm>.

[482] idem, *Chicago Summit Declaration* (issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012) para 49 <http://www.nato.int/cps/en/SID-D03EFAB6-46AC90F8/natolive/official_texts_87593.htm?selectedLocale=en>.

7. Summary and Conclusions

Cold War metaphors with regard to cyberspace appear as a facet of nostalgia for the bipolar, relatively predictable political environment of those times, where 'fronts' were apparent and concepts of the enemy clear. In the cyber context, any simple recipe would fail, facing as it would the complex realities of today's world, where cyber tools empower non-State actors and politically unstable and otherwise militarily inferior States. Herewith, the usual search for power balance between the global players, which traditionally would lead to relative security in international relations, is not useful, as cyberspace empowers the weak ones and leaves the technically advanced 'Great Powers' particularly vulnerable. For diverse reasons as demonstrated in the present paper, the adoption of an arms control regime for cyber means or the conclusion of an international agreement on State behaviour in cyberspace are at the present neither practicable nor politically feasible. Against this background, the elaboration of CBMs within the fora of the UN and OSCE, as a proposal for adoption at a wider international level, are the viable option, as they focus rather on process than on values. The development of a joint position of NATO member States on CBMs for cyberspace or conducting a thorough study about the applicability of CBMs to cyberspace within NATO's *Science for Peace and Security Programme* would certainly support the work of the international community. In any case, it could be beneficial for the organisation to closely observe respective developments, especially as occurring in the fora of other international organisations, e.g., by the delegation of observers.

Due to specific characteristics of the internet, traditional CBMs referring to specific weapons, to geographic areas (of demilitarisation), to limitations of military manoeuvres or to any kind of verification and control are not feasible. Also, CBMs referring to military spending, otherwise a useful indicator for the defensive or offensive orientation of a State, are not practicable in the cyber realm, as cyber capabilities are characterised by skills and knowledge rather than the equipment purchased. Also, the situation for the development of CBMs for cyberspace is very different from the environment, in which traditional disarmament negotiations take place, as States do not have the monopoly or control over production and import of malicious software.

Thus, CBMs which predominantly refer to transparency (information-sharing) and cooperation are feasible for cyberspace. A comparison of the available sets of (draft) CBMs for cyberspace with sets of 'traditional' CBMs referring to transparency and cooperation clearly shows that CBMs for cyberspace, as currently discussed, present a minimum of possible political commitments. This reflects the level of controversy surrounding governmental cyber activities, and might additionally be affected by the different levels of sophistication of States with regard to the development of cyber infrastructure, national cyber security frameworks, and the role cyberspace plays in administration, industry and civil society. However, there might be value in the fact of the elaboration of the first CBMs for cyberspace, which can serve as a basis for future developments in that arena.

The value of legal obligations is the possibility to take legal remedies (such as countermeasures) in cases of their breach which, in any case, requires a clear attribution of the supposed violation of the norm to a State. The attribution, of which a threefold concept was presented, will very seldom occur in a form which would satisfy the evidentiary rules of international law. As the lack of attribution would make any allegation of a treaty breach impossible, and thus any treaty-based obligation futile, the international community focuses their endeavours on the development of CBMs as politically binding measures.

The aforementioned challenge of attribution as well as the secrecy surrounding offensive cyber capabilities of States does not necessarily limit the effectiveness of CBMs as political commitments, as is claimed especially with regard to the 'transparency' aspect of CBMs. Although the anonymity of action within the internet minimises the political risk of States (with regard to political retaliation), sociological and philosophical studies show that, where assurance is low and risk of disappointment is high, trust (as opposed to assurance) tends to show a higher level of intensity. However, one of the obstacles to the effectiveness of CBMs for cyberspace is that malicious cyber tools are foremost an asymmetric and powerful means in the hands of 'super-empowered angry individuals'. Another impediment is the fact that the adopted, recommended or currently negotiated CBMs do not consider the potential of de-escalation of certain non-State actors, such as tier 1 ISPs, who would first notice irregular data streams or malicious software, and undertake crisis management measures. An 'isolationist' approach at the international level could eventually shift the international cyber crisis management to global, informal cooperation fora such as FIRST. All in all, in preparation for the negotiations of CBMs for cyberspace, it would be recommended to conduct an in-depth study on the applicability of CBMs to cyberspace, as elaborated in 1993 in the context of CBMs for outer space. Additionally, an analysis of lessons identified with regard to CBMs, as collected by armed forces and peace research institutes during the last decades, would be beneficial in order to consider the findings during the current negotiations with regard to cyberspace.

Political declarations are a powerful tool of international relations, which can have *de facto* binding character (good faith, estoppel). Furthermore, the political discourse within the international community can support the development of international customary law by facilitating the evolvement of *opinio iuris*, which is (beside State practice) a constitutive aspect of international custom. Furthermore, political declarations can support the interpretation of international law norms of rather general character. Additionally, as CBMs are discussed at the international level as a 'substitute' for legally binding obligations, they could show the character of 'soft law', thus being 'in the twilight between politics and law', and showing some normative value.

Currently, only a few international treaties can be deemed as reflecting measures as enclosed in the sets of (draft) CBMs for cyberspace. Cyber-specific regulations of customary law, of general principles deriving from municipal laws, of legally binding decisions (or recommendations) of international organisations or unilateral acts of States invoking legal obligations are hitherto not detectable. However, cyberspace does not present a legal *lacuna*, but is governed by general principles of international law.

General principles of international law can be derived, *inter alia,* from general considerations, legal logic, legal relations in general, international relations, or from a particular treaty regime. Hitherto, neither international courts nor academia have developed a methodology for identifying the principles. However, with regard to general principles of international law as pertaining to international peace and security, international courts and academia acknowledge the existence of several principles based on sovereign equality of States, the duty to the maintenance of international peace and security, and the duty to international cooperation in solving international problems. These principles (and their sub-principles or correlating principles) are endorsed in Article 1 and 2 of the UN Charter and confirmed by the UNGA *Friendly Relations Declaration*, as well as, for example, by the *Helsinki Declaration*. General principles of international law may serve different purposes, of which the most significant is the function as a basis for the progressive development of international law, responding to rising extra-positive needs of the international society, such as the 'emergence' of cyberspace as a common space for inter-State relations.

Sovereignty, although strongly affected by interdependence, globalisation, and the emergence of international organisations, among others (which is especially true for cyberspace, introducing vertical and diagonal relations between all stakeholders), is the core of the notion of statehood and an axiomatic principle upon which international law is based. The following obligations and rights of States can be deemed as deriving from the equal sovereignty of States, and from principles respectively de-conflicting the competing sovereign rights within the international community:

- Based on legal logic, no State can claim sovereignty over the global resource that is the internet or the common space of cyberspace. This finding is supported *de lege ferenda* by the principle of common concern of humankind.
- Based on the principle of territorial sovereignty, a State may regulate for its own territory internet activities (also with regard to contents) of its own or foreign nationals conducted on its territory or showing effects on its own territory. States need especially to consider human rights law with regard to the right to access to the internet.
- Based on the principle of territorial sovereignty, the duty not to harm other States' rights, the principle of good neighbourliness and the *sic utere tuo* principle, a State is forbidden to cause physical effects to technical components of the internet located on the territory of another State or to cause other effects relevant to the national security of the affected State.
- Based on the preventive principle deriving from the 'no-harm rule', the principle of good neighbourliness and the *sic utere tuo* principle, States have the obligation to prevent malicious cyber activities which harm or could harm the rights of other States, and thus to:
    - ensure that national ISPs install network sensors collecting information on the 'net flow', i.e., amount of routed data (allowing to detect, e.g., 'DDoS attacks'),

- ensure that national tier 1 ISPs install intrusion detection/prevention systems at their 'gates' of international data transmission, conducting deep package filtering (allowing recognition of malicious software),
- establish a respective reporting system of ISPs to a governmental entity (e.g., a national or governmental CERT),
- establish a respective framework of strategic, political, legal, administrative, organisational and technical nature allowing to conduct the above-mentioned measures as well as to ensure effective management of prevention of malicious cyber activities potentially harming other States' rights (including risk assessment, as well as notification and information of and consultation with other States),
- establish investigative cyber capabilities (allowing the identification of the source of the malicious cyber activities),
- establish an organisational and legal framework allowing the prevention or discontinuation of concrete malicious cyber activities originating on the State's territory and potentially harming the rights of other States.

- Based on the precautionary principle (deduced from the legal regimes governing global resources and common spaces) or on a 'due diligence' principle (derived from the 'no-harm' rule), as well as on the principle of good neighbourliness and the *sic utere tuo* principle, States are obliged to establish a national cyber security framework. This finding is supported *de lege ferenda* by the principle of sustainable development of global resources, and by the principle of common concern of humankind.
- Based on the preventive principle deriving from the 'no-harm rule', the principle of good neighbourliness and the '*sic utere tuo*' principle, States are obliged to inform, notify, and consult other States in situations of concrete cyber incidents which are likely to cause physical damage in the territory of other States or any other effects relevant to the national security of other States.
- Based on the principle of (territorial) jurisdiction, States shall not conduct online law enforcement activities (e.g., online search) in networks located on another State's territory. However, such activities do not violate the principle of non-intervention in domestic affairs of another State, as the element of 'coercion' is not present.
- Based on the duty to cooperate and on the principle of solidarity, States are obliged to establish and maintain an intensified cooperation in the cyber realm. Due to the principle of (competing and overlapping) jurisdiction, States shall cooperate closely in law enforcement activities in cyberspace. This results in the obligation of the establishment of the organisational, legal and (investigative) technical framework for cyber law enforcement in the realm of international cooperation.
- The principle of non-intervention in domestic affairs of another State is not violated with regard to political demands related to internet communication as such, access to internet, or cyber security, as these areas do not belong to the purely internal affairs of a State.

- Based on the duty to maintain international peace and security, States are obliged to attempt to seek a solution by peaceful means with regard to any question involving the cyber realm.
- Based on the duty to maintain international peace and security, States are obliged to refrain from the use of force by cyber means. This finding is supported *de lege ferenda* by the principle of common concern of humankind.
- *De lege ferenda*, based on the principle of equitable utilisation of shared resources and on the principle of common concern of humankind, States should establish an internationalised, just and fair regime for the worldwide distribution of IP addresses.
- *De lege ferenda*, authorities similar to those which the WHO deploys with regard to globally spreading infections (and diseases), as contained in the IHR, could be applied to cyberspace, empowering an international entity to adopt regulations on cyber incidents reporting, quarantine requirements for networks, nomenclatures of malicious software, standards of cyber security, standards of purity of software, advertising and labelling of software, and taking emergency measures in cases which require immediate action.

The above interpretation of general principles of international law, as far as it refers to cooperation in concrete cases of cyber incidents and in the arena of law enforcement, as well as to the establishment of a national cyber security framework, is supported by the CBMs as recommended by the UN GGE or as currently negotiated within OSCE, which reflect what the participating States consider as politically acceptable. These (draft) CBMs refer explicitly to law enforcement cooperation and cooperation in addressing security incidents. They also presuppose the existence of CERTs (e.g., by proposing respective exchange of contact data) and partly also of a national cyber security framework (e.g., by proposing the exchange of respective documents or contact data of responsible personnel at technical and political levels). Though, the (draft) CBMs do not reflect any obligations deriving from several other general principles of international law, e.g., from the duty to an intensified cooperation. This is, however, conditioned by the specific goal of CBMs to prevent the outbreak of war or (international) armed conflict by accident.

Interestingly, the sets of (draft) CBMs do not reflect the duty to refrain from the use of force in international relations. Although States in general prefer to maintain a strategic ambiguity with regard to questions related to use of force and armed attack, thus leaving the respective debate to academia, it would certainly support predictability and stability in international relations if they shared their views on aspects of the 'use of [armed] force' in cyberspace, 'armed attack' and preventive self-defence in cyberspace, non-State actors as potentially triggering the right to self-defence, and the 'accumulation of events' or *Nadelstichtaktik* theory with regard to malicious cyber activities. Also, States should clarify the role of the armed forces towards ISPs and CERTs of industry providing critical infrastructure, which will conduct concrete defensive measures on a 'bit for byte' basis in the case of an 'armed attack' targeting such infrastructures.

It should be noted that general principles of international law are recognised as a normative source of law, either as part of international customary law or as a separate source of international law. Following a specification of their contents by interpretation, as proposed in the present paper, general principles of international law achieve the quality of a 'hard law' obligation or of a right of a State.

Importantly, due to their nature as the foundation of the international law system, it is widely recognised within scholarly writings that such general principles of international law pertaining to international peace and security, as presented above, are essential for the 'co-existence and vital co-operation of the members of the international community', and thus exist, irrespective of a State's *opinio juris* practice, consent or any other expression of the will of a State. Moreover, such basic principles enjoy a 'heightened' normativity because of their *quasi*-constitutional role within the international law system or as peremptory norms of international custom. This results in the most important finding: States cannot 'opt-out' from basic general principles of international law.