CYBER SECURITY ACADEMY

Cyber Confidence-Building Measures

Ten stumbling blocks which complicate the development and implementation of worldwide politically acceptable cyber confidence-building measures

Kraesten Arnold
2016

Master Thesis – MSc. in Cyber Security
Cyber Security Academy, The Hague
Kraesten Arnold, s8245312
Supervisor: Sergei Boeke LL.M.
Second reader: Prof dr Jan van den Berg M.Sc.
Date: November 25, 2016
Word count: 23,998 (excl. abstract, preface, annexes and references)

Abstract

Cyber attacks can form a threat to international peace and stability. Many of such cyber attacks may well be state-sponsored or state-driven and carry the risk of an unintended escalation into an inter-state armed conflict. A system of confidence-building measures may help prevent destabilisation and help ensure worldwide confidence in cyberspace. To date, such measures have only materialised to a limited extent. This paper identifies ten stumbling blocks that complicate the development and implementation of worldwide politically acceptable *cyber* confidence-building measures.

Preface

This thesis concludes a part-time academic executive master's program 'Cyber Security' of the Cyber Security Academy The Hague. This program has started in January 2015 and was developed by Leiden University, Delft University of Technology and The Hague University of Applied Sciences and various private partners. The multidisciplinary program covered technological as well as legal, administrative, economic and psychological aspects of digital security.

The subject of my thesis originated in the program's governance track that focused, among other things, on governance theories related to cyber threats and security, the implications of cyberspace on interstate relations, (inter)national law and regulation, as well as moral and legal issues, and dilemmas. As staff member of the Netherlands Armed Forces' Defence Cyber Command I am directly involved in the development and use of cyber weapons and tools by state actors. Moreover, I am fully aware of the potential risks that cyber attacks, incidents, weapons and warfare pose to our global society. Therefore, I also realise that the development and implementation of measures that could limit such risks, is of paramount importance.

As regards the research for this thesis, I would like to express my very warm thanks to all diplomats, researchers and other experts whose opinions, experience and advice proved to be invaluable resources to my ideas, survey, analysis and eventual report. Without short-changing anyone, I would like to especially thank Caítriona, Rutger, Tobi, Sico and Patryk. Furthermore, I would like to express my sincere thanks for the support that I have received from my family, colleagues and friends: Maaike, Maroussia, Giovanni, Hans, and Arthur, thank you very much for your time, patience and valuable comments.

Finally, I would like to express great appreciation to all Cyber Security Academy core and guest lecturers for their inspiring stories, activities and lectures. Last, and certainly not least, I would like to express my deep appreciation and gratitude to my two supervisors, Professor Dr Jan van den Berg, M.Sc., and Sergei Boeke LL.M., for the manner in which they motivated, supported, advised and criticised me throughout this final academic project. It has been a real joy and honour to work with you.

Kraesten Arnold
Cyber Security Academy, The Hague

November 25, 2016

Table of Content

1. Introduction

In his opening speech at the 2015 global conference on cyber security in The Hague, Dutch Minister of Foreign Affairs Bert Koenders stated "We are living in a complex security environment, both physically and virtually. It is clear that cyber attacks can form a threat to international peace and stability. We need to set up a system of confidence-building measures that can help prevent destabilisation and help ensure confidence in cyberspace worldwide."[1]

One year later, during the February 2016 cyber roundtable at the 'Münchner Sicherheitskonferenz' in The Hague, Koenders portrayed his opinion on the contemporary dependency on cyber infrastructure and the growing vulnerability to cyber incidents and attacks. Somewhat disappointed he concluded that the challenges had not been diminished, but rather increased.[2] Apparently, while states are saying one thing by making international agreements, they continue to behave in a different manner. The minister expressed his fear that many of such cyber attacks may well be state-sponsored or state-driven.[3] He reiterated the need for cyber diplomacy to develop a framework that specifies norms and that regulates state behaviour in cyberspace.[4] Koenders called for global action to prevent escalation and urged not to await a 'cyber 9/11'.[5]

1.1. Dependence on IT and OT. Modern society is increasingly interconnected and interdependent. National professional and social networks are intertwined with other national and international networks and systems. The free flow of data and unhindered functioning of network structures have become vital for states and non-states, businesses and individuals. The increasing reliance on the stable and secure functioning of information technology (IT) and operational technology (OT) – the hardware and software dedicated to monitoring and controlling physical devices mainly used in industrial control systems and/or critical infrastructures – has created significant new vulnerabilities and threats to societies. Digital networks and systems have thus become crucial to states, the worldwide economy, our wider society and our individual daily lives.

Many business sectors rely on the proper functioning of network and information systems of both IT and OT. According to the EU Commission, some sectors (e.g., energy, information and communication technology, transport, finance, and health) provide key services and are therefore crucial to a well-functioning society and economy. Consequently, the security of these vital infrastructures is also of paramount importance.[6]

Network and information security has become increasingly important to our economy and society. Moreover, the EU Commission declared it a precondition for worldwide trade in services.[7] Unintentional and deliberate security incidents (e.g., technical failures, human errors or cyber attacks) could have a negative effect on networks and information systems. These security incidents are becoming bigger and occur more frequent, whilst being more complicated.[8]

[1] Bert Koenders, *Opening speech*, Global Conference on Cyber Security, The Hague, April 16, 2015. Accessed May 4, 2016, https://www.government.nl/documents/speeches/ 2015/04/16/opening-speech-gccs-bert-koenders
[2] Bert Koenders, *Speech at the Münchner Sicherheitskonferenz*, The Hague, February 12, 2016, Accessed July 2016, https://www.rijksoverheid.nl/documenten/toespraken/2016/02/12/toespraak-van-minister-koenders-munchner-sicherheitskonferenz
[3] Idem.
[4] Idem.
[5] Idem.
[6] EU Commission, *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Rev 2, 2013/0027 (COD), Brussels, 18 December 2015, p 4.
[7] Idem, p 2.
[8] Ibidem.

1.2. Cross-border cyber incidents may affect peace and stability. Although the cyber domain is often dependent on physical means (i.e. computers, networks, servers, routers), it is in principle largely unaffected by the existing geographical state borders.[9] As cyber activities allow local, regional or even global operations, cyber actors can reach effects way beyond their own state borders, and thus have a potential negative impact on international peace and stability. Cyber actions can be initiated at one place and achieve simultaneous effects in multiple other places; worldwide. A major disruptive cyber incident originated in one state carries the risk of misperception by another state having the impression that it is under attack. This might lead to unintended escalation into cross-border armed conflicts, and could thus seriously affect international peace and stability.[10]

1.3. Deliberately destabilising cyberspace. A variety of state and non-state actors operate on the internet for various reasons.[11] State actors operate in cyberspace according to specific state duties and responsibilities as regulated by international law. However, in addition to this regulated type of behaviour, during peacetime states also demonstrate, knowingly allow or condone specific unlawful behaviour on the internet. According to the 'Tallinn Manual', military cyber operations involve "the employment of cyber capabilities with the primary purpose of achieving military objectives in, through or by cyberspace."[12] Particularly state actors involved in 'cyber war' could thus *deliberately* destabilise cyberspace. During peacetime, state actors may already 'prepare the cyber battlefield' and/or collect intelligence, thereby behaving in ways where it may not be easy to distinguish their intentions between traditional espionage and possible conflict. States' intentions may thus be difficult to ascertain.

1.4. No cyber wars? "Cyber war will not take place"[13] wrote Thomas Rid in his 2012 eponymous article. Rid claims that "cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future."[14] To put it bluntly, in the same vein, a pure sea, land or air war will not take place either. A nice thought: where there is no threat of war, we need not fear its risk. Where there is no threat of cyber war, we need not fear a deliberately destabilised cyberspace. Or should we? Rid refers to Von Clausewitz's[15] three principles of war to argue that cyber war would imply (1) an act of force conducted through malicious computer code having a possible lethal impact. In addition, such a cyber war needs to be (2) instrumental and (3) politically driven.[16] In the absence of all three conditional principles, Rid concludes that all politically motivated cyber attacks are merely sophisticated versions of sabotage, espionage or subversion. Consequently, according to Rid, these cyber attacks are not considered as cyber war.[17] Then what is?

1.5. Cyber warfare. The 'Tallinn Manual' defines a cyber attack – or cyber warfare – as a cyber operation, whether offensive or defensive, which is reasonably expected to cause injury or death to persons, or damage or destruction to objects.[18] Cyber warfare can be seen as an armed attack when

[9] I.e. geographical borders still exist and infrastructure lies within sovereign states, but data transport may occur worldwide, cross-border ignoring the actual state borders.
[10] ASEAN Regional Forum on Operationalising Confidence Building Measures for cooperation during cyber-incident response, *Concept-paper*, Kuala Lumpur 2-3 March 2016, p 1.
[11] Ministry of Security and Justice, National Cyber Security Centre, *Cyber Security Assessment Netherlands (CSAN) 2015*, The Hague, The Netherlands, November 2015, p 27 – 31.
[12] Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare* prepared by the international group of experts at the invitation of the NATO cooperative Cyber Defence Centre of Excellence: Cambridge University Press, 2013, p 258.
[13] Thomas Rid, *Cyber War Will Not Take Place*, Journal of Strategic Studies (2012), 35:1, 5-32. Accessed August 2016, DOI: 10.1080/01402390.2011.608939.
[14] Idem, p 5.
[15] Carl von Clausewitz, *Vom Kriege: hinterlassenes Werk*, Frankfurt/M, Berlin, Wien: Ullstein 1832, (1980).
[16] Rid, *Cyber War Will Not Take Place*, Journal of Strategic Studies, 35:1, 5-32, p 5.
[17] Idem, p 5.
[18] Schmitt, *Tallinn manual*, Rule 30, p 6.

executed by cyber means,[19] or as any activity involving the use of computer code to achieve military objectives.[20] In 2014, NATO concluded that cyber-attacks or cyber warfare may indeed be similar to conventional warfare. The NATO alliance recognised that article 5 – the collective self-defence principle – can be invoked in cases where a cyber attack would achieve effects similar to conventional armed attacks.[21] Rids (pure) 'cyber war' may perhaps not take place. Cyber attacks, however, might indeed be internationally interpreted as an act of armed conflict or (cyber) warfare.

1.6. Confidence-building measures for cyberspace. Such cyber activities carry the risk of an unintended escalation into an interstate armed conflict. To date, however, worldwide accepted and legally binding treaties, laws or norms concerning state behaviour in cyberspace, are lacking. The international community has concluded that existing international law, and in particular the Charter of the UN, is applicable to cyberspace.[22] According to Pawlak, the guidelines on *how* the existing international law should actually be interpreted are just starting to come into sight.[23]

As regards war and warfare, the law of armed conflict (LOAC) describes various restraints and constraints, but does not particularly involve cyber-elements. It is not yet clear whether the unique characteristics of cyberspace would justify a specific 'cyber law of armed conflict', or if further clarification under the LOAC would suffice. However, in the current absence of a specific 'cyber law of armed conflict', a common understanding of cyber activities as worldwide threat and global challenge to international peace and security, has led to the ambition to develop politically binding confidence-building measures (CBM) for cyberspace.[24] There is a clear need for strengthening international cooperation to ensure that a major cyber incident can be dealt with. Hitherto, however, these measures have only materialised to a certain extent. This raises the question as to why worldwide politically acceptable *cyber* confidence-building measures (CCBM) have not yet been developed and implemented.

1.7. States in cyberspace. State actors and their proxies involved in malicious cyber activities, cyber attacks or cyber warfare may intentionally destabilise cyberspace. In addition to official (state) and semi-official (proxy) bodies, also non-official (non-state) actors, such as the Islamic State, other terrorist organisations or Anonymous,[25] may carry out intentionally destabilising actions. State policies and behaviour *also* shape and influence international relations and agreements. The fact that worldwide politically acceptable CCBM have not yet been developed and implemented may thus be the result of particular state behaviour or willingness; or the absence thereof. Many factors influence state behaviour, such as politics, religion, culture, ethnicity, law, economy or social issues. Many actors, with various perceptions of national, organisational or personal interests, may frame problems, specify alternatives, and push proposals towards their government and thus influence state behaviour.[26]

[19] US Vice Chairman or the Joint chiefs of Staff, *Joint Terminology for Cyberspace Operations*, 2010-11, Attachment 1, Cyberspace Operations Lexicon, p 8.
[20] Kraesten Arnold and Arthur Dalmijn, *Working paper in preparation of The Netherlands Doctrine for Military Cyber Operations,* draft Netherlands Ministry of Defence restricted version, August 2016, p 7.
[21] NATO, *Wales Summit Declaration*, September 2014, Accessed August 2016, http://www.nato.int/cps/en/natohq/official _texts _112964.htm.
[22] UN document A/68/98, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, p 2.
[23] Patryk Pawlak, *Cyber Diplomacy: Cyber-Confidence-Building Measures*, European Parliamentary Research Service, Members' Research Service PE 571.302, briefing to the European Parliament, October 2015.
[24] Katharina Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2013, p 11.
[25] Anonymous is an informal international network of activists and 'hacktivists'; see also: http://anonhq.com/
[26] Graham T. Allison, *The American Political Science Review*, *Conceptual models and the Cuban missile crisis*, Volume 63, Issue 3 (Sep 1969), p. 689-719. DOI: http://dx.doi.org/10.2307/1954423.

Various actors with different conceptions of international, national or organisational goals have different, coloured perceptions on 'what must be done'. Although final decisions about CCBM are taken at the highest political level – governments eventually decide – these governments do not hold absolute power over every CCBM-facet. Moreover, governments actually share their power among various other groups, such as commercial businesses, NGOs or other interest groups. Whereas once the Internet was considered a borderless world, according to Deibert, cyberspace has become a hotly contested and deeply politicized realm.[27]

1.8. Purpose and scope of this paper. Given the need for strengthening international cooperation to ensure that a major cyber incident does not escalate and leads to an international conflict, this research paper seeks to answer the following question:

> *'Which are the stumbling blocks that complicate the development and implementation of worldwide politically acceptable Cyber Confidence Building Measures?'*

Although various actors are able to destabilise cyberspace, the focus in this paper lies on state actors and their proxies, as they could be directly involved in cyber warfare and, consequently, deliberately destabilise cyberspace. Furthermore, as mainstream interlocutor state actors are also involved in, and responsible for, international relations, peace and stability, and, consequently, the development and implementation of interstate confidence-building. In order to answer the main research question, various sub-questions are derived, divided into three sub-areas:

A. Domain exploration and analysis
   (1) What are a state's duties and responsibilities in cyberspace?
   (2) Who are the state actors and their non-state proxy actors in cyberspace?
   (3) How do state actors and proxies behave and act in cyberspace?
   (4) What state behaviour is jeopardising international peace and stability?
   (5) What is the influence of cyberspace on international relations?
B. Cyber Confidence Building Measures
   (6) What are confidence-building measures?
   (7) Which endeavours to develop and implement cyber confidence-building measures have been made to date?
C. Obstacles
   (8) Which are the obstacles that hamper worldwide agreement on worldwide politically acceptable cyber CBM?

1.9. Methodology and structure. To answer the main and sub-questions, an exploratory qualitative desk and field research has been conducted in the natural science tradition. The research intends to determine the nature of the identified problem in order to better understand the current challenges, without presenting conclusive solutions. To that end, existing literature on this subject has been studied to firstly explore and analyse the domain, in order to understand and describe why and how state actors and proxies show certain behaviour in cyberspace. Furthermore, the existing literature has been studied to discover and comprehend the influence of cyberspace on international relations. A literature study has also been conducted to collect, analyse and subsequently assess various relevant cyber confidence-building initiatives, and to identify possible obstacles to the creation and implementation of CCBM.

[27] Ronald J. Deibert, *The geopolitics of internet control: Censorship, sovereignty, and cyberspace*, in *The Routledge handbook of internet politics* (2009), edited by Andrew Chadwick and Philip N. Howard, Part 4, Chapter 23, p 324.

In addition to the aforementioned desk research, national and international conferences, symposia and meetings were attended. Discussions and (unstructured) interviews with individual diplomats and researchers and focus groups of appropriate experts were held, and observations were made, to confirm, deny or examine the identified potential obstacles to worldwide acceptable CCBM. On the basis of the initial desk and the additional field research, an analysis was conducted to identify why the current measures appear to be insufficient and/or not acceptable to states, and to recognize the stumbling blocks that actually hamper the development or implementation of worldwide politically acceptable CCBM. To validate the research and associated conclusions, this paper has been peer reviewed by national and international experts.

This paper comprises three main parts of which the first major part relates to the domain exploration and analysis; it answers the aforementioned sub-questions 1 to 5. To that end, initially state duties, tasks and responsibilities in cyberspace are clarified. Thereafter, the various state actors and non-state proxy actors are identified. Furthermore, particular state behaviour and actions that endanger cyberspace is described. The final section examines the influence of cyberspace on international relations. As confidence-building measures are usually developed and implemented in the context of international politics, this paper highlights the influence that cyberspace exercises on international relations.

With a clear view on what a state may do, or rather does in cyberspace, and which actors execute the according tasks or perform certain jeopardising actions, the second main part of the paper then answers sub-questions 6 and 7. First, the origin of the general confidence-building measures (CBM) and the differences between military and non-military CBM are examined. Thereafter, a recent history of CBM is presented and a brief introduction to the UN guidelines for CBM is given. This is followed by a more extended view on the work that the organisation for security and cooperation in Europe (OSCE) has done and is still doing in this area. In particular, attention will be paid to the OSCE's practical 'guide on non-military confidence-building measures'.[28] This part then continues with a focus on cyber, presenting various multilateral, regional and bilateral endeavours to develop and implement *cyber* CBM.

The final major part of this paper discusses the difficulties concerning global and politically acceptable cyber confidence-building measures and provides an overview of the ten stumbling blocks that actually complicate the development and implementation of CCBM. This paper ends with some conclusions, a recommendation and an additional reflection.

[28] OSCE *Guide on Non-Military Confidence-Building Measures (CBMs)*, Organization for Security and Co-operation in Europe, Vienna, 2012. Accessed August 2016, http://www.osce.org/cpc/91082?download=true.

2. States' duties, responsibilities and behaviour in cyberspace

Although cyberspace goes beyond the internet and everything that is connected to it,[29] according to The Netherlands Scientific Council for Government Policy, the internet in general, and its core of key protocols and infrastructure in particular, may well be considered a global public good.[30] Merely recognising the internet as a global public good is not sufficient to counter the growing state interference with the internet.[31] Before concentrating on confidence-building measures, it is essential to first explore and identify the domain, i.e. to identify which duties, responsibilities and authority states have in cyberspace, and what constitutes actual state actors' behaviour that could jeopardise cyberspace. To that end, existing literature on this subject has been studied.

This chapter first describes the set of rules that serves as framework for international relations between states. It also explains why enforcing the rules is a challenge, especially in cyberspace. Thereafter, the perceived absence of cyber-specific laws is raised, followed by an explanation of the common set of general principles of international law that apply in the absence of particular (cyber) laws. This section is followed by an overview of the various state actors in cyberspace, and their proxies. The part thereafter describes various types of actual state behaviour that may jeopardise cyberspace. Furthermore, the influence of cyberspace on international relations is analysed. This chapter ends with a sub-conclusion.

2.1. Framework for interstate relations. The set of rules that serves as framework for international relations between states and nations is legislated in international law (e.g., treaties, customary international law, judicial decisions or general international law).[32] Much of this international law, however, is based on the basic principle of 'the consent to be bound'.[33] This permission is an issue of state sovereignty. Consequently, a state is not obliged to abide by this type of international law,[34] unless is has specifically consented to do so. The driving idea behind this principle is that when a state consents with a certain law, in case of a dispute, this state is also (more) likely to submit to judgements of supervisory bodies.[35] One of the challenges in international law is the fact that in most cases a body to enforce the rules is absent. In the case of an international armed conflict the UN Security Council (UNSC) may authorise the use of force to maintain or restore international peace and security,[36] but the UNSC has no standing forces at its disposal. Acting against violation of the rules is, therefore, often left to individual states. Whereas enforcing agreed international law has been challenging in other ('actual world') fields hitherto, creating rules that serve as framework for interstate relations in (the 'virtual world' of) cyberspace, will be equally challenging.

---

[29] Netherlands *National Cyber Security Strategy 2, from awareness to capability*, Ministry of Security and Justice, National Coordinator for Security and Counterterrorism, The Hague, The Netherlands, 28 October 2013, footnote p 7: Cyberspace or 'the digital domain' is the conglomerate of ICT tools and services and comprises all entities that can be or are digitally linked. The domain comprises both permanent, temporary or local connections, as well as information, such as data and program codes, located in this domain where geographical limitations do not apply.

[30] Dennis Broeders, *The public core of the Internet,* An international agenda for Internet governance, Amsterdam: Amsterdam University Press, 2015, p. 9.

[31] It is worth noting that there are no worldwide accepted cyber terms, definitions or interpretations. The given definitions are primarily a Dutch understanding. There may well be other understandings of these definitions and the debate as to whether these are global public goods or global commons.

[32] Anthony Aust, *Handbook of International Law*, London School of Economics and Kendall Freeman Solicitors, Cambridge: Cambridge University Press, 2005, p 5 - 11.

[33] Willem J.M. van Genugten, *Handhaving van wereldrecht: Een kritische inspectie van valkuilen en dilemma's*. Nederlands Juristenblad, (2010) 85(1), p 44.

[34] A UN Security Council resolution is an exception to this rule, as UN Charter art 25 states that all UN Member States must accept and execute the Security Council's decision. From: Willem van Genugten, '*Handhaving van wereldrecht: Een kritische inspectie van valkuilen en dilemma's'*. Nederlands Juristenblad, (2010) 85(1), p 44.

[35] Van Genugten, *Handhaving van wereldrecht*, p 44.

[36] United Nations Security Council, http://www.un.org/en/sc/

2.2. The perceived absence of cyber-specific laws. According to Ziolkowski, some claim that cyberspace is not, or is only partly, regulated by law as cyber-specific international custom is absent, and as there is only little contractual regulation.[37] In such a situation, however, the following basic principle would be applied. On the basis of sovereignty a state enjoys freedom of action with the exception of legally explicitly prohibited actions.[38] The perceived absence of cyber-specific laws, however, does not imply that states can enjoy unlimited freedom of action in cyberspace. The freedoms of competing sovereign states are rather guided and de-conflicted by various general principles of international law. According to Ziolkowski, these general principles are relevant to cyberspace as they form the basis for the creation of international cyber-specific laws.[39]

2.3. Three general principles of international law. Ziolkowski indicates that a common set of general principles of international law as relevant to international peace and stability is acknowledged.[40] This set of principles[41] encompasses three main elements: (1) the sovereign equality of states; (2) the maintenance of international peace and security, and (3) the duty to international cooperation in solving international problems.[42] In the absence of cyber-specific laws pertaining to international peace and security, these general principles thus serve as a basis for the development of such laws. This is especially the case for the rapidly evolving cyberspace that affects the current inter-state relations.[43]

Furthermore, as the general principles pertaining to international peace and security are considered as a prerequisite for the well-being and well-functioning of the international community, these principles will apply irrespective of a state's action, *opinion iuris*,[44] or will.[45] Hence, these general principles serve, and are applied, as international 'law' regardless states' individual opinion. The next section describes the characteristics of the three main, and various derived, principles and assesses their application to cyberspace.

2.4. First general principle of international law: Sovereign equality of states and four derived principles**.** Most, if not all principles of international law, directly or indirectly rely on state sovereignty.[46] This principle ensures the juridical (not political, military, economic, geographic, demographic or other) equality of states.[47] Because of, among other things, globalisation, the acknowledgment of international organisations' decisions as a potential source of international law, the growing interdependence of states, and the understanding that states are obliged to promote and safeguard common values and goals of the international community, the notion of sovereignty has

[37] Katharina Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, in *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski, NATO CCD COE Publication, Tallinn, 2013, p. 135.
[38] As Stated in 1927 by the Permanent Court of International Justice (PCIJ) in the *Lotus* case, cf The Case of the S.S. 'Lotus', Merits (1927) PCIJ Rep Ser A, No 7, 18ff; Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 135.
[39] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 135.
[40] Idem, p 185.
[41] Endorsed in Article 1 and 2 of the UN Charter, Ziolkowski, *General Principles of International Law as Applicable in Cyberspace* p 185.
[42] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 143-144.
[43] Idem, p 185.
[44] In customary international law, opinio juris is the second element (along with state practice) necessary to establish a legally binding custom. Opinio juris denotes a subjective obligation, a sense on behalf of a state that it is bound to the law in question. See ICJ Statute, Art 38(1)(b) (the custom to be applied must be 'accepted as law'). https://www.law.cornell.edu/wex/opinio_juris_international_law
[45] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 156.
[46] Samantha Besson, *Sovereignty* in MPEPIL (n 2) MN 2; cf Epping and Gloria (n 143) § 26 MN 13.
[47] Pierre d'Argent and N. Susani. *United Nations, Purposes and Principles*, in *The Max Planck Encyclopedia of Public International Law*, edited by Rüdiger Wolfrum, Oxford University Press, online edition, (n 105) 11.

changed in character.[48] As a result of these aspects, sovereignty has transformed from the traditional Westphalian view on a state's independency,[49] to a relative concept.

Although in parts of the world the internet is state-owned, large parts of the internet have grown into a worldwide, largely privately owned and driven network. The various political, economic and social networks on the internet are interlinked. Cyberspace is characterised by numerous visible and invisible (interwoven and mutual dependent) links between the public and private sector, international corporations, societies and individual people.[50] Yet, in cyberspace too, state sovereignty is the leading principle of international law. On the basis of state sovereignty, four derived sovereignty principles are identified.[51]

2.4.1. First sovereignty principle: self-preservation. The first principle that is based upon sovereign equality of states is self-preservation or the fundamental right to survival, thus to self-defence in situations of an 'armed attack' launched by another state (or possibly by non-state actors).[52]

An 'armed attack' or the 'use of force'[53] does not imply the use of specific weaponry, and can thus be conducted also by electronic means (i.e. computer code, a cyber weapon). Labelling an electronic operation as 'armed attack' rather depends on the assessment of the scale and effects of that attack.[54] Consequently, on the basis of this self-preservation principle, malicious cyber activities which could be considered as an 'armed attack' against a state might result in a military response (in self-defence). The right to self-preservation entails also the right to take protective measures when necessary.[55] Whether the right to self-preservation also includes the right to anticipatory self-defence (i.e. pre-emptive action) is a controversial question that reveals a wide disparity of opinions.[56]

2.4.2. Second sovereignty principle: territorial sovereignty and jurisdiction. The second principle derived from the sovereign equality of states involves territorial sovereignty, including the principle of jurisdiction.[57] With regard to cyberspace this aspects stands for exercising full and exclusive authority over a territory, as well as protecting the 'cyber infrastructure' that is located on a state's territory or is otherwise under its exclusive jurisdiction.[58] Von Heinegg emphasises that territorial jurisdiction also applies to hardware components that are situated within a state's territory, but that are simultaneously part of the worldwide internet.[59]

Von Heinegg also indicates that any act from one state resulting in physical impact on another state's territory is considered a violation of the latter state's territorial sovereignty.[60] A well-known example of a cyber activity that caused actual physical damage, and thus violated the territorial sovereignty of

[48] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace,* p 156.
[49] The formulation of sovereignty was one of the most important intellectual developments leading to the Westphalian revolution. Accessed September 2016: http://www.wwnorton.com/college/polisci/essentials-of-international-relations5/ch/02/summary.aspx
[50] Idem p 157.
[51] Idem p 157 – 170.
[52] UN Charter, Chapter VII, Article 51: *Action with respect to threats to the peace, breaches on the peace, and acts of aggression.*
[53] UN Charter, Chapter I, Art. 2(4).
[54] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace,* p 158.
[55] Idem p 162.
[56] Christopher Greenwood, *Oxford International Public Law,* Max Planck Encyclopedia of Public International Law [MPEPIL], Self-Defence, Anticipatory Self-Defence, art. 41-51, retrieved from: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e401
[57] Ibidem.
[58] Wolff Heintschel von Heinegg. *Legal Implications of Territorial Sovereignty in Cyberspace,* in *Proceedings of the 4th International Conference on Cyber Conflict,* edited by Christian Czosseck, Rain Ottis and Katharina Ziolkowski, NATO CCD COE Publication (2012) p 7, 10 and 13.
[59] Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace,* n 200, p 14.
[60] Idem p 16.

a state, is the malicious software (malware) called 'Stuxnet'. Stuxnet was first identified in 2010[61] and appeared to be a complex piece of malware; a worm[62] designed to attack the computers that control Iran's nuclear enrichment centre at Natanz. As it caused the physical destruction of objects, Richardson argues that Stuxnet has risen to the level of an armed (cyber) attack under international law.[63] In a study on this particular attack,[64] twenty independent legal experts unanimously confirmed that Stuxnet was an 'act of force'.[65] The experts' views diverged on whether this 'cyber sabotage' act actually constituted an 'armed attack'.[66]

As malicious cyber activities could also generate significant *non-physical*, nonetheless visible, effects, these effects could also violate a state's sovereignty. Malicious cyber operations that negatively affect, for example, a state's critical infrastructure[67] (either physically or non-physically) are thus also considered a violation of territorial sovereignty. An example of such an attack on a state's critical infrastructure is the 2015 'BlackEnergy3' cyber attack on three Ukrainian electricity distribution companies, leading to power outages.[68]

Another cyber activity that affects a state's sovereignty is (cyber) espionage. Espionage, however, appears to be internationally condoned. There is currently neither a specific international treaty that regulates cyber espionage, nor is there any specific international treaty which could be adapted to control such practices. Nevertheless, Buchan emphasises that cyber espionage may be unlawful when it contravenes the general principles of international law (i.e., in particular the principles of territorial sovereignty and non-intervention are also applicable to espionage in cyberspace).[69]

Oxman explains that the jurisdiction principle comprises a state's power to develop, implement and enforce laws, and to manage the behaviour of juridical and natural persons. The jurisdiction principle is usually limited to a state's own territory. A state has jurisdiction over the creation of national laws and regulations, and the law-enforcing reactions in case of a violation thereof.[70] The principle of jurisdiction would be violated when foreign state actors conduct activities in networks and comput-

[61] Stuxnet is believed to be a jointly built American-Israeli cyber-weapon, but neither state has confirmed this openly. Stuxnet was first discovered in 2010 by Sergey Ulasen, at the time the head of a small and obscure security company in Minsk, called 'VirusBlokAda'. From: Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, in Wired Magazine, November 7, 2011. Accessed October 8, 2016, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/1

[62] A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. From: http://searchsecurity.techtarget.com/definition/worm

[63] John C. Richardson, *Stuxnet as Cyberwarfare Applying the Law of War to the Virtual Battlefield*, Social Science Research Network, 2011.

[64] This study was produced by a group of 20 independent legal experts (under the direction of lead author Michael Schmitt) at the request of NATO's Cooperative Cyber Defense Center of Excellence in Estonia. From: Kim Zetter, *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*, in Wired magazine, March 25, 2013. Accessed October 8, 2016, https://www.wired.com/2013/03/stuxnet-act-of-force/

[65] Kim Zetter, *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*, in Wired magazine, March 25, 2013. Accessed October 8, 2016, https://www.wired.com/2013/03/stuxnet-act-of-force/

[66] Ibidem.

[67] Physical or virtual systems and assets such as under the jurisdiction of a State that are so vital that their incapacities or destruction may incapacitate a State's security, economy, public health, or safety, or the environment (e.g.: financial, electricity, health, water, transportation sectors).

[68] The 'BlackEnergy3' malware was used to carry out a cyber attack on Dec 23, 2015 on three regional Ukrainian electricity distribution companies which resulted in power outages. BlackEnergy3 is believed to be (Russian) state-sponsored malware, but to date, full-proof for this accusation has not been found. From: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf and Kim Zetter, Everything We Know About Ukraine's Power Plant Hack, in Wired magazine, January 20, 2016, Accessed October 8, 2016 from: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

[69] Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, in *International Cyber Norms, Legal, Policy & Industry Perspectives*, edited by Anna-Maria Osula and Henry Rõigas, NATO CCD COE Publications, Tallinn 2016, p 68.

[70] B.H. Oxman, Jurisdiction of States, in The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, Oxford University Press, online edition, (n 2) MN 3. Accessed August 2016, http://opil.ouplaw.com/home/EPIL.

ers located on another state's territory without prior consent of the other state or outside cooperation frameworks.[71] Ziolkowski remarks that particularly with regard to cyber-crime law enforcement, there may be an overlap in the jurisdiction of various states.[72]

2.4.3. Third sovereignty principle: non-intervention. A third sovereign equality-related principle involves the principle of 'non-intervention'. Gill notes that this expression denotes that states may not interfere with the internal (or external) affairs of other states.[73] According to Ziolkowski, a coercive act is considered as an illegal intervention when a state interferes with the 'internal' affairs of another state in order to force the latter to change its behaviour.[74] Although Heinl emphasises that some would argue that the internet is *not* a global commons/globally shared resource,[75] Ziolkowski considers the internet a globally shared resource.[76] As malicious software is spread worldwide too, aspects of national cyber-security must be considered as of internationalised interest, and fall, therefore, outside of the realm of purely 'internal' affairs.[77]

To violate the principle of non-intervention there must be coercion, hence illegal influence (as opposed to legal, i.e. political or economic, influence).[78] Ziolkowski explains that influencing will only be considered coercive, and thus illegal, only when states put an overwhelming force upon another state in order to influence its free and sovereign decision-making process.[79] Online law enforcement activities of foreign agencies, for example, would probably not be deemed 'coercive';[80] and even less when the host state gives another state permission to carry out such actions.

2.4.4. Fourth sovereignty principle: duty not to harm the rights of other states. As stated by Ziolkowski, the fourth sovereign equality-based principle involves the duty not to harm the rights of other states and consequently, not to let its own sovereign territory be used for activities causing damage to persons or objects protected by the sovereignty of another State.[81] This 'no-harm principle' also means that a state has the obligation to take preventive measures in cases where that state has the knowledge or the presumption of an actual risk of harm to other states, whereas that risk is originating from their own sovereign territory.[82]

Furthermore, states are also obliged to take precautionary measures with regard to cyber threats posing a significant international cross-border risk.[83] Additionally, the fourth principle includes 'due diligence' of states regarding malicious cyber activities of *non-state* actors originating from the state's territory and harming the rights of other states.[84] Whereas the prevention principle means that states must inform other states in cases of significant trans-boundary harm, the precautionary and 'due diligence' principle imply that measures must be taken well before such risk of harm occurs.

2.5. Second general principle of international law: maintenance of international peace and security. Maintaining international peace and security is one of the United Nations' (UN) main pur-

[71] Idem, p 47.
[72] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 164.
[73] cf Terry D Gill, 'Non-Intervention in the Cyber Context' and Chris Demchak, 'Economic and Political Coercion and a Rising Cyber Westphalia' in Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, (n 212), p 164.
[74] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 164.
[75] As set out in her peer review comments, Caitriona H. Heinl, Caitríona H. Heinl, Research Fellow, Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.
[76] It must be noted that some (e.g., would argue that the internet is not a global commons/globally shared resource.
[77] Idem, p 165.
[78] Ibidem.
[79] Ibid.
[80] Ibid.
[81] Idem, p 165-166.
[82] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 166.
[83] Idem, p 167.
[84] Idem, p 168.

poses.[85] Peace should not only be regarded as 'an absence of war', but also means that possible threats to peace and security should be removed or mitigated. The development and implementation of confidence-building measures may also contribute to peace.[86] The two principles derived from this basic principle imply that (1) in international relations states refrain from the use of force, or threatening to do so, and (2) states shall seek to resolve any international dispute in a peaceful manner.[87] In this case the term 'force' is to be understood as 'armed force', but not limited to 'military weaponry'.[88]

With regard to the term 'use of (armed) force' in cyberspace, according to Schmitt, there is a general agreement on the idea that the effects of an action determine whether or not (armed) force has been used.[89] As Randelzhofer and Dörr put it, when the use of 'cyber-weapons' results (directly or indirectly) in death or injury to people, or severely disrupts the critical infrastructure or the economy of a state,[90] the use of such 'cyber-weapons' is considered as 'use of (armed) force'. This cyber-weapon approach has been adopted by the group of academics that has written and compiled the 'Tallinn manual on the international applicable to cyber warfare'.[91] Ziolkowski indicates that illegal copying and the destruction of data are thus not regarded as 'use of (armed) force', as in these cases deadly or devastating direct or indirect effects are absent.[92]

As unsettled disputes might lead to an unstable and insecure international community, the obligation to peacefully settle international disputes links with the prohibition of 'the threat or use of force'. Tomuschat argues that, when a state perseveres in refusing to at least try to settle the international dispute it is involved in, such a stance is considered to be a violation of the principle of maintaining international peace and security.[93] With regard to cyberspace, according to this principle, states involved in an international dispute must therefore try to settle their disagreement irrespective of the issue, without resorting to the use of (armed) force.

2.6. Third general principle of international law: cooperation and solidarity. Whereas there is a general consensus on the previous principle, according to Ziolkowski, there is a dispute concerning the existence of a legal basis and a general duty to cooperate.[94] The current globalisation, the interdependence of states, the vast number of intergovernmental organisations and international treaties, as well as the endorsement of the duty of cooperation in the UN Charter do indicate 'the general duty to cooperate' as normative.[95]

States have an obligation to cooperate as far as it supports the maintenance of international peace and security; also in the realm of cyberspace.[96] The term 'cooperation' itself, however, is vague as it

[85] UN Charter, Chapter 1, Art 1, purposes and principles.
[86] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 172.
[87] Ibidem.
[88] Ibid.
[89] 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) 885, 913 and 919; Stein and Marauhn, (n 238) 6.
[90] A. Randelzhofer, and O. Dörr, *Article 2(4)* in *The Charter of the United Nations* 3rd edition, volume 1, edited by B. Simma et al., Oxford University Press, 2012, p 43.
[91] […] "For the purpose of this Manual, cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack (Rule 30)". Michael N. Schmitt, (ed.), *Tallinn manual on the international law applicable to cyber warfare* prepared by the international group of experts at the invitation of the NATO cooperative Cyber Defence Centre of Excellence: Cambridge University Press, 2013, Rule 41 – 2, p 141 – 142.
[92] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 174.
[93] C. Tomuschat, Article 2(3) in *Oxford Commentaries on International Law, The Charter of the United Nations*, 3rd Edition Volume 1, edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus and Editor Nikolai Wessendorf (assistant editor), Oxford University Press, 2012, p 25.
[94] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 176.
[95] Ibidem.
[96] Idem p 177.

is not defined by an international treaty or in another multilateral document.[97] Cooperation can be perceived as the voluntary and proactive joint action of two or more states which serves a specific objective in the interest of the international community.[98] The second part of this principle, solidarity, could be seen as a more far-reaching form of cooperation, mainly on the basis of shared values and common interests.[99]

Although Heinl notes that others have counter-arguments and thus different positions,[100] according to Ziolkowski (supported by The Netherlands Scientific Council for Government Policy),[101] cyberspace has evolved into a common space which is in the interest of the international community.[102] Cyberspace has also led to the present worldwide interdependency. This justifies the concept of cooperation and solidarity. Consequently, states have a legal obligation to cooperate to reduce cyber activities that threaten international security. However, states have a wide discretion as to how to fulfil that legal obligation.[103]

2.7. State actors and proxies in cyberspace. The previous section explained states' duties and responsibilities in cyberspace, expressed in principles that are mainly based upon equal sovereignty of states. Yet another principle is drawn from the sovereignty principle, namely the state's monopoly on the use of (physical) force, or rather the state's monopoly on the legitimate use of (physical) violence.[104] Although various sources of power exist (e.g., diplomatic, information, military or economic), the legitimate use of violence is the only source of power that is confined to the state's privilege. With regard to cyberspace, Czosseck defines the term 'cyber power' as "the ability to act and influence through, and by means of, cyberspace."[105] State actors may conduct operations[106] in cyberspace to exercise (cyber) power. Consequently, state actors may use cyber means to legitimately exert violence. The next section identifies the main categories of state actors and proxies, and their respective activities in cyberspace.

2.8. State actors. States may vary in, among other things, political ideology, cyber capabilities, norms, state behaviour, and cyber actors with unique tasks and authorities that are specific to a particular state (e.g., the Cyberspace Administration of China (CAC),[107] the Iranian Cyber Police).[108] There are, however, three main categories of cyber state actors that are rather similar among all states: (1) law enforcement, (2) intelligence services, and (3) armed forces. Although unique state actors may exercise a lot of cyber power, to limit the scope of this study, only the three groups of common state actors are successively discussed in the paragraphs below.

---

[97] Ibidem.
[98] Ibid.
[99] Idem p 178.
[100] As set out in her peer review comments, Caitriona H. Heinl, Caitríona H. Heinl, Research Fellow, Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.
[101] Dennis Broeders, *The public core of the Internet*, An international agenda for Internet governance, Amsterdam: Amsterdam University Press, 2015, p. 9.
[102] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 178.
[103] Ibid.
[104] The legitimate use of force is widely regarded as a defining characteristic of the modern state. The term was introduced by the German sociologist Max Weber in his lecture 'Politics as a Vocation' (1918), in which he defines the state as a 'human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory'. From: Encyclopaedia Brittannica, https://www.britannica.com/topic/state-monopoly-on-violence
[105] Christian Czosseck, *State Actors and their Proxies in Cyberspace*, in P*eacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn, 2013, p 1.
[106] The term 'cyber operations' refers to "[t]he employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace". From: Schmitt, *Tallinn manual*, p 258.
[107] The Cyberspace Administration of China (also: 'the Office of the Central Leading Group for Cyberspace Affairs'), is involved in cyber security and internet information, http://www.cac.gov.cn/english/
[108] Cyber Police Islamic Republic of Iran is involved in monitoring Iranians' online activities and the prosecution of dissidents. J. Alex Halderman, *Internet Censorship in Iran: A First Look*, https://jhalderm.com/pub/papers/iran-foci13.pdf

2.8.1. Law enforcement. At present, cyber-crime is organised professionally and the possibilities provided by the internet are often used to make other forms of criminality possible.[109] In 2011, a Norton cyber-crime study estimated that "cyber-crime costs the world more than the global black market in marijuana, cocaine, and heroine combined."[110] In 2016, Forbes estimates the cost of global cyber-crime about $2.1 trillion by the year 2019.[111] Next to securing the society and providing security for the individual citizen, according to Czosseck, one of the fundamental goals of a state is to ensure national security. This type of security usually includes enforcing the rule of law and/or protecting citizens from crime.[112] Czosseck estimates that, albeit to different degrees, many states already possess the technical means and skills to investigate cyber-crime, and have the power to enforce the law and pronounce sanctions in cyberspace.[113]

Czosseck also argues that, although some of the modern law enforcement structures are widely accepted and easy to implement (e.g., computer forensics and open source intelligence), many states have also introduced more controversial, innovative, high-tech applications in the area of communication and computing, such as, for instance, the ability to intercept and decode encrypted communication.[114] There are various ways to get access to encrypted data. States might use their regulatory power over industries operating in their territory and legally demand unencrypted access to all data. Furthermore, states could install listening software (i.e. malware) on a suspect's communication devices. Although some states can develop their own malware, most of the law enforcement agencies do not posses the necessary skills, knowledge or means to produce the required malware and depend on legal or illegal businesses to produce such software.[115] When fighting cyber-crime, law enforcement agencies might thus use the very same technologies and methods as cyber criminals, however, with proper legitimacy, and aiming for different purposes.[116]

2.8.2. Intelligence services. Espionage between states is a common and rather traditional activity which is an internationally tolerated state practice, although generally criminalised in national legal systems.[117] Czosseck argues that, due to its worldwide interconnectivity, cyberspace has further facilitated espionage and interception. Consequently, many states have developed capabilities for online espionage, data and document interception, or any other information or activity of interest.[118]

Intelligence services make use of malicious software programmes to get access to classified digital data and information for various purposes, such as: monitoring, surveillance, extracting or modifying data to change the system configuration or to take down the entire system. The underlying reasons range from diplomacy, national security, to strategic or economic benefits.[119] Intelligence services could thus abuse IT infrastructures on a large scale for their cyber operations, i.e. digital attacks on, or intrusions in other states. Espionage may well be an internationally tolerated state practice; it also poses a significant threat to states' national security.

---

[109] Ministry of Security and Justice, National Cyber Security Centre, *Cyber Security Assessment Netherlands (CSAN) 4 - 2014*, The Hague, The Netherlands, October 2014, p 24.
[110] Norton Cybercrime Report, *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually*, Symantec Press Release, September 7, 2011. Accessed April 28, 2016, https://www.symantec.com/about/newsroom/press-releases/2011/symantec_0907_02.
[111] Forbes business and financial website, Accessed November 25, 2016, http://www.forbes.com/forbes/welcome/?toURL=http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/&refURL=https://www.google.nl/&referrer=https://www.google.nl/
[112] Czosseck, *State Actors and their Proxies in Cyberspace*, p 12.
[113] Ibidem.
[114] Idem p 12-13.
[115] Idem p 13.
[116] Ibidem.
[117] Idem p 14.
[118] Ibidem.
[119] Markus Maybaum, *Technical Methods, Techniques, Tools and Effects of Cyber Operations*, in *Peacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, p 104.

2.8.3. Armed forces. In 2007, Farivar noted that the term 'cyber war' was often being used to describe a wide variety of malicious activities in cyberspace, ignoring the actual meaning of the term 'war' (being an armed conflict). The term 'cyber war' just seemed to thrive well in the media.[120] Nevertheless, the first 'cyber wars' were openly declared. In 1988, the US hacker group 'Legions of the Underground' declared a 'cyber war' on Iraq and China.[121] The second 'cyber war' was declared during East Timor's struggle for independence against the occupation force Indonesia.[122] In the end, both 'cyber wars' were never fought. Despite the often referred to cyber incidents in Estonia (2007) and Georgia (2008), in the meaning of an armed conflict a 'cyber war' has not yet taken place.[123] The Ukraine conflict (2013) also showed cyber activities as part of hybrid warfare, but again there was no 'pure cyber war'. Rid's claim that cyber wars have not taken place thus still stands.[124] Nevertheless, according to NATO, cyber attacks may be interpreted as (cyber) *warfare*.[125]

The incidents in Estonia, Georgia and Ukraine have led to an international discussion as to 'if and how' to consider cyberspace as yet another military domain for warfare. Whereas various states,[126] including the Netherlands, have officially declared cyberspace as fifth domain for warfare,[127] Songip argues that many scholars dispute whether or not cyberspace may be recognised as new and really different domain for warfare.[128] Moreover, as cyberspace is a man-made domain, one could even question to what extent it is useful to actually describe cyberspace as a fifth domain other than practically useful for military doctrine and operational planning. However, even without officially recognising cyberspace as a domain for military operations, various states have built or are developing offensive military cyber capabilities and are introducing these into their military doctrines. States may use such cyber capabilities against other state or non-state actors. To date, the use of offensive military cyber operations may yet seem limited (e.g., the US dropping 'cyber bombs' on ISIL[129] in support of their more traditional weaponry),[130] but future potential impact might well be significant.[131]

According to the United Nations institute for disarmament research (UNIDR), in 2011, about 32 states included cyber warfare in their military planning and organisations.[132] The US, China and Russia are well known and commonly recognised for having developed offensive cyber warfare capabilities.[133]

---

[120] Cyrus Farivar, *A Brief Examination of Media Coverage of Cyberattacks* (2007 - Present), in *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Cristian Czosseck & Kenneth Geers, Amsterdam: IOS Press. doi:10.3233/978-1-60750-060-5-182, pp. 182-188.
[121] On December 29, 1988 the Legions of the Underground (LoU) called for a full-scale destruction of computer systems, because these countries' governments allegedly violated human rights. From: Albert Benschop, *Cyberoorlog, slagveld internet*, Tilburg, Uitgeverij de Wereld, 2013, p 189.
[122] Albert Benschop, *Cyberoorlog, slagveld internet*, Tilburg, Uitgeverij de Wereld, 2013, p 191.
[123] James Andrew Lewis, *The Cyber War Has Not Begun*, Center for Strategic and International Studies (CSIS), March 2010. Accessed July 2016, http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf
[124] Thomas Rid, *Cyber War Will Not Take Place*, Journal of Strategic Studies (2012), 35:1, 5-32. Accessed August 2016, DOI: 10.1080/01402390.2011.608939.
[125] NATO, *Wales Summit Declaration*, September 2014, Accessed August 2016, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.
[126] Such as the USA and the UK.
[127] These five domains are land, sea, air, space and cyberspace. NATO also recognises cyberspace as a domain of operations in which it must defend itself as it does in the air, on land and at sea, http://www.nato.int/cps/en/natohq/topics_78170.htm
[128] Ahmad Rahman Songip et al., *Cyberspace: The Warfare Domain*, World Applied Sciences Journal 21 (1): 01-07, 2013. ISSN 1818-4952, IDOSI Publications, 2013, DOI: 10.5829/idosi.wasj.2013.21.1.2825, p 1.
[129] The Islamic State of Iraq and the Levant.
[130] David E. Sanger, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, in The New York Times, April 24, 2016, accessed October 9, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=1
[131] Ministry of Security and Justice, National Cyber Security Centre, *Cyber Security Assessment Netherlands (CSAN) 4 - 2014*, The Hague, The Netherlands, October 2014, p 23.
[132] Czosseck, *State Actors and their Proxies in Cyberspace*, p 15.
[133] Ibidem.

2.9. Proxies. Various reasons could lead to states making use of proxy actors. An obvious reason is that a state merely lacks the required skills, knowledge or means to operate in cyberspace. Another reason for using proxy-units is related to political (un-) willingness to openly employ state actors or in cases where state cyber activities would not match with the state's legal, ethical or cultural norms. Proxies may then be used for defensive, offensive or intelligence gathering activities. An additional benefit is that a cyber operation carried out by a proxy-unit complicates the unambiguous attribution of that activity. It is thus difficult to prove a state's liability for such cyber activities.

Using proxies, however, does not mean that states are not responsible for a proxy's activities. Moreover, from a legal point of view, Schmitt notes that states are not just responsible for cyber activities that are carried out by state entities or cyber activities that can otherwise be attributed to states.[134] Moreover, actions of non-states actors might also well be attributed to states.[135] Consequently, certain proxy-actions may fall under state responsibility.

A range of proxy actors has been active in the recent conflict between Russia and Ukraine,[136] for both defensive and offensive purposes. Russian hacker groups executed Denial-of-Service (DoS) attacks and carried out defacements, thereby triggering a DoS-retaliation from Ukrainian patriotic hacker groups such as 'Cyber Hundred' and 'Null Sector'.[137] The NATO alliance also used the service of a proxy actor, the Rumanian state-owned company Rasirom,[138] to train and improve the Ukraine's cyber defences. In addition, various other hacktivist groups have carried out offensive cyber activities for either side of the warring factions.[139]

2.10. State behaviour jeopardising international peace and stability. The previous sections showed which state actors and proxies operate in cyberspace and what their generic activities are. The next paragraphs focus on the aspects that could potentially endanger international peace and stability in, though or by cyberspace.

2.10.1. Anonymous operations. As cyberspace allows certain levels of anonymity that makes attribution a forensic and time-consuming challenge, state actors, state-sponsored and non-state actors may exploit these vulnerabilities to conceal their true identity or intentions. As the attribution problem give states the ability to deny responsibility,[140] this type of state behaviour contributes to creating misperception. Unverified reports, false allegations and thus erroneous attribution may even further complicate this issue.

In 2014, a cyber attack took place on Sony Pictures. The company's (confidential) data was stolen (rather: illegally copied), partly dumped onto public file-sharing sites, and partly destroyed.[141] The US federal bureau of investigation (FBI) pointed at North Korea as the alleged perpetrator of this

[134] Schmitt, *Tallinn manual on the international law applicable to cyber warfare*, p 15.
[135] Ibidem.
[136] The conflict between Ukraine and Russia was the result of political tension that escalated in 2013, when former Ukrainian president Viktor Yanukovych abandoned plans to sign a trade agreement with the EU. From: Tim Maurer, *Cyber Proxies and the crisis in Ukraine*, Chapter 9 in *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by Kenneth Geers, NATO CCD COE Publications, Tallinn 2015, p 80.
[137] Tim Maurer, *Cyber Proxies and the crisis in Ukraine*, Chapter 9 in *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by Kenneth Geers, NATO CCD COE Publications, Tallinn 2015, p 80 – 81.
[138] Idem, p 84.
[139] i.e., pro-Kyiv OpRussia, Russian CyberCommand, Cyber Ukrainian Army, Cyber Hundred, Null Sector, and the pro-Moscow CyberBerkut and Anonymous Ukraine. From: Maurer, *Cyber Proxies and the crisis in Ukraine*, in *Cyber War in Perspective: Russian Aggression against Ukraine edited by Kenneth Geers*, p 85.
[140] Thomas Rid and Ben Buchanan, *Attributing Cyber Attacks*, Journal of Strategic Studies 38 (2014): 4-37, retrieved from: https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf
[141] Peter Elkind, *Inside the hack*, Fortune Special Investigation Report, Fortune Magazine (online version), Accessed August 2016 http://fortune.com/sony-hack-part-1/

hack, which was denied by the latter.[142] Various journalists and cyber security experts remained sceptical and openly doubted the US accusation that North Korea was behind the hack.[143] [144]An additional challenge is that competent hackers can spoof an identity and thus shift the suspicion of a malicious action to another identity. To date, a variety of state and non-state actors have been appointed as the alleged perpetrator, (i.e., North Korea, Russia, China, the US, the FBI, (Sony) insiders, hacktivists, and the (cyber criminal) Lazarous Group).[145] Even if firm and objective evidence is available to attribute the operation to the actual culprit, the question is whether that evidence would be published, as that would probably also reveal how, where and by whom that evidence has been collected – secret and/or even illegal according to international law. Potential serious and credible evidence thus remains hidden. Not being able to provide credible and actionable evidence to the international community implies that sanctions or other forms of retaliation will be harder to accept by the international community. As states can deny their responsibility, anonymous cyber operations may thus contribute to misperception.

2.10.2. Cyber espionage. Another action that states may conduct in cyberspace is collecting, processing, analyzing, and using data for a variety of reasons. These data could be obtained from open sources or, in the case of classified information, gathered by means of unauthorised access, also known as intelligence gathering or espionage. Information can be gathered in a traditional way: on spot by conventional secret agents or insiders, whilst in the cyber-version hackers may steal classified information from a distance, using computers, networks and malicious software. As there are no international treaties that prohibit these practices, (cyber) espionage and (cyber) intelligence gathering are tolerated. An additional benefit is that the data stored in cyberspace holds many secrets that range from industrial, commercial and infrastructural interests to diplomatic, political and (national) security interests. According to Buchan, cyber espionage may be easily conducted with a fairly limited risk,[146] due to the seemingly blurred geographical state borders in the cyber realm as well as the large degree of anonymity that cyberspace provides for entities that are associated with espionage.

The fact that states are engaged in espionage is of all times. Intelligence tactics, techniques, procedures and operations were carried out well before cyberspace was created. Cyber espionage, however, is relatively new. In 2009, China has stolen (i.e. illegally copied) terabytes of data related to the design and electronic systems of the US Joint Strike Fighter project.[147] In 2013, Canadian researchers revealed that they had found real-time evidence of a cyber espionage network based mainly in China that had hacked into computers and documents from governments and private organisations in 103 countries.[148] In 2014, cyber security company FireEye published a report in which they claimed to have found sufficient evidence to assess a long-standing espionage effort in (Eastern) Europe – executed by the Russian hacker group 'Advanced Persistent Threat 28' (APT28) – as being sponsored by the Russian government.[149] This APT28 cyber espionage effort was assessed to be aimed at

[142] David E. Sanger, Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, The New York Times, December 17, 2014. Accessed August 2016 http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0
[143] Post Staff Report, *New evidence Sony hack was 'inside' job, not North Korea*, New York Post, December 30, 2014. Accessed October 14, 2016, http://nypost.com/2014/12/30/new-evidence-sony-hack-was-inside-job-cyber-experts/.
[144] Kim Zetter, *The evidence that North Korea hacked Sony is flimsy*, in Wired Magazine, December 17, 2014. Accessed October 14, 2016, https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/; http://www.canada.com/entertainment/movie-guide/Security+experts+doubt+North+Korea+hacked+into+Sony+regime+angry+over/10434868/story.html.
[145] *What is known about the Lazarous Group*. Accessed August 2016, https://blog.kaspersky.com/operation-blockbuster/11407/
[146] Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, in *International Cyber Norms, Legal, Policy & Industry Perspectives*, edited by Osula and Rõigas, p 66.
[147] Wendell Minnick, *Chinese businessman pleads guilty of spying on F-35 and F-22*, in *Defense News*, March 24, 2016, Accessed October 14, 2016, http://www.defensenews.com/story/breaking-news/2016/03/24/chinese-businessman-pleads-guilty-spying-f-35-and-f-22/82199528/
[148] Fox News article, *Cyber Spy Networks Hacks Computers in 103* Countries, March 30, 2009. Accessed October 14, 2016, http://www.foxnews.com/story/2009/03/30/cyber-spy-network-hacks-computers-in-103-countries.html
[149] FireEye, Special Report, *APT28: A Window into Russia's Cyber Espionage Operations*? p 28, Accessed October 14, 2015. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

collecting intelligence on defence and geopolitical issues since at least 2007.[150] In 2013, the American cyber security firm Mandiant identified China as a perpetrator of massive cyber espionage against other states and non-state actors. The report describes the existence of 'Unit 61398', a newly created division of the Chinese People's Liberation Army specialised in cyber espionage.[151]

Both China and Russia are often accused, usually by the US, of carrying out cyber espionage activities, but they appeared to be not the only culprits. In June 2013, former contractor for the US national security agency (NSA) Edward Snowden disclosed thousands of classified documents to the media. The documents revealed that also the US (i.e. the NSA) had been engaged in a global surveillance programme – in, by and through cyberspace – to collect confidential information about numerous state and non-state actors.[152] Entities involved in cyber espionage need to conduct operations in a stealthy manner using skills, techniques and means that make the targeted cyber systems and networks inherently insecure. Once offensive cyber activities have been discovered and incidents have, whether or not correctly, been attributed and assessed, escalation is lurking.

2.10.3. The use of proxies. A relatively unregulated cyberspace and deficiencies of international cooperation facilitate cyber-crime and 'hactivism'. A state might prefer to outsource its cyber activities and use proxies, such as cyber criminals, patriotic hackers or other capable non-state actors, for actions that other states might consider hostile acts. These state-sponsored or state-supported proxies can thus be used *inter alia*: to informally carry out state missions; as a source for recruitment; or to develop specific cyber technologies. In addition, proxies could be employed to exercise pressure on other parties that a state does not favour. They may also carry out notable, yet misleading cyber activities with the purpose of distracting the attention from other, stealthier cyber activities that a state wishes to conceal.[153] What these proxies have in common, is that they support a state's goals (i.e. financial gain or a shared ideology).[154]

The 2016 US democratic national committee (DNC) cyber hack, in which some 20,000 DNC-internal communication emails were stolen and subsequently published,[155] has allegedly been executed by Russian state-sponsored proxies.[156] The technical evidence (e.g., the tools that were used, IP-addresses, language, location settings) would clearly point in the direction of the Russian government's involvement.[157] However, in this incident too, the attribution problem exists. Gayken argues that technical evidence can be spoofed; the cyber tools that have been used earlier by some known Russian proxies may have been recycled and reused by another actor; and language and location settings could easily have been changed.[158] In those cases, other sources of intelligence, such as human intelligence, have an equally important role in attributing cyber attacks.

While state actors are managed by governments, private actors are more difficult to control as they cannot be monitored or held directly accountable in the same ways as state actors.[159] When it comes

[150] Idem, p 3.
[151] Ibidem.
[152] Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, p 66.
[153] Idem p 18.
[154] Idem p 19.
[155] Some 20,000 DNC internal communications emails were hacked and subsequently published on Wikileaks in July 2016. From: Matthijs Veenendaal et al., *DNC Hack: An Escalation That Cannot Be Ignored,* NATO CCD COE News Article, August 5, 2016. Accessed August 2016, https://ccdcoe.org/dnc-hack-escalation-cannot-be-ignored.html.
[156] "Based on the analysis by Crowdstrike (and corroborated by Fidelis Cybersecurity and Mandiant) there is convincing evidence that hackers closely associated with the Russian government were behind the attacks on the DNC." From: Matthijs Veenendaal et al.. *DNC Hack: An Escalation That Cannot Be Ignored*.
[157] Sandro Gayken, *Blaming Russia For the DNC Hack Is Almost Too Easy*, August 1, 2016, Accessed August 2016, http://blogs.cfr.org/cyber/2016/08/01/blaming-russia-for-the-dnc-hack-is-almost-too-easy/.
[158] Ibidem.
[159] Jordan Brunner, *Iran Has Built an Army of Cyber Proxies*, in *The Tower Magazine*, Issue 29, August 2015. Accessed October 14, 2016, http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/

to supporting and employing cyber proxies, according to Brunner, Iran appears to be a major user of such proxy entities.[160] In addition to its own, state-regulated cyber army (the Iranian Revolutionary Guard Corps claimed to have built the fourth biggest cyber power among the world's cyber armies),[161] Iran also sponsors the cyber-capabilities of various proxy units (e.g., terrorist organisations in Lebanon, Yemen and Syria).[162]

Ironically, FBI's accusation of North Korea being the mastermind behind the earlier mentioned Sony hack is based on state hackers *not* always using proxy *servers*.[163] On multiple occasions, the hackers would have failed to use their proxy servers that ought to have redirected their internet connection to computer addresses elsewhere in the world. As a result, according to the FBI, forensic investigation has revealed IP-addresses that led directly to North Korea. The challenge with proxy servers is, however, that it is hard to prove that those IP-addresses are 'real', and not proxies themselves, leading to even more deception.[164] Consequently, in such cases attribution by other means of intelligence, in addition to cyber forensic investigation, is absolutely necessary.

The complicated combination of state actors, acting through proxy actors using proxy servers, results in a forensic, attribution and accountability challenge. While there is an accountability challenge, thanks to other intelligence sources some states (e.g., the United States of America) have experienced that technical attribution is becoming less difficult. Nevertheless, proving particular intent and showing the actual evidence to the international community remains difficult.

2.10.4. Military cyber capabilities for offensive purposes. The skills, knowledge and means that are necessary for cyber defensive purposes are rather similar to the tactics, techniques, procedures and means that are used to carry out offensive cyber activities. Offensive efforts, investments or cyber-weapons are thus easy to deny and easy to conceal. Indeed, offensive cyber units cannot be monitored as easily as traditional military units. Furthermore, compared to conventional war machines (e.g., battle tanks, warships and combat aircraft) offensive cyber knowledge and means are easily obtainable and relatively inexpensive. This makes cyber weapons particularly suitable for asymmetric warfare.[165]

The options for offensive cyber purposes grow proportionally with the increasing use of state-of-the-art technologies within armed forces. This constitutes a significant risk of proliferation of such cyber capabilities. In 2011, about 32 states had adopted the cyber warfare option.[166] Only four years later, a Wall Street Journal research estimated that already more than 60 states have or are developing means for cyber attack or cyber espionage.[167] Jellenc recognises the existence of "a global cyber arms race."[168]

---

[160] Ibidem.
[161] Ibidem.
[162] Ibidem.
[163] Andy Greenberg, *FBI Director: Sony's 'Sloppy' North Korean Hackers Revealed Their IP Addresses*, in *Wired Magazine*, July 1, 2015, Accessed October 15, 2016, https://www.wired.com/2015/01/fbi-director-says-north-korean-hackers-sometimes-failed-use-proxies-sony-hack/.
[164] Ibidem.
[165] The more technologically sophisticated a state or an army is, the more vulnerable it is to cyber attacks, whereas an attacker only needs a laptop, some software and an internet connection to threaten and harm his adversary.
[166] Czosseck, *State Actors and their Proxies in Cyberspace*, p 15.
[167] Wall Street Journal article from October 11, 2015. The Wall Street Journal consulted public sources, computer security experts and researchers to compile estimates. From: http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710
[168] Eli Jellenc, *Explaining the Global Cyber Arms Race: Strategic Rivalry and Securitization of Cyberspace among Nation-States*, in The Proceedings of the 11th European Conference on Information Warfare, Laval, France, July 6-7, 2012. Accessed August 2012 from: http://www.academia.edu/7664607/Explaining_the_Global_Cyber_Arms_Race_Strategic_Rivalry_and_Securitization_of_Cyberspace_among_Nation-States.

Cyber weapons can be used for 'information warfare' (e.g., to influence a population, for psychological warfare or strategic communications), but they can also be used for more destructive attacks. The fact that purely military networks and systems are possible targets for military cyber warfare is fairly obvious. However, every digital object is a potential target for a cyber attack. The possibility that structures with a civil/military ('dual-use') function, or entirely civilian critical infrastructures, could be targeted too, or at least might be affected by a cyber attack, is perhaps less obvious. Although, according to the LOAC, these non-military objects *should* not be targeted, they still *could* be harmed; either deliberately, or unintentionally (as collateral damage or as the result of a second or third order (side) effect). Cyber capabilities for military purposes – cyber warfare – may thus also jeopardise civilian objects and structures. Consequently, they may have a harmful impact on international peace and stability. This negative effect may be aggravated when such offensive cyber activities are carried out anonymously or by proxy actors, or when the attacks have far-reaching cross-border impact.

As stated earlier, there is general agreement that Stuxnet can be considered as an 'act of force', but not necessarily as an 'armed attack'. The worldwide development of cyber weapons is still in its infancy. This certainly applies to deadly and destructive cyber weapons. Since the discovery of Stuxnet in 2010, there have been a few (known)[169] other cyber attacks serving military purposes.[170] These cyber attacks were mainly executed by non-state proxy actors against civilian state-targets and particularly used as first-strike weapon or supporting action with limited, non-decisive effects.[171] Yet, the Stuxnet worm has shown the potentially lethal and devastating impact that (future) cyber weapons possibly have.

2.10.5. Knowingly allowing and condoning malicious activities. Malicious behaviour can be shown by state-actors or their (state-sponsored or –supported) proxies, but malevolent cross-border activities could also be conducted by private parties (e.g., hacktivists, criminals or terrorists). According to Pirker, the challenge then is how to determine the precise extent to which a state is accountable for, and could thus be obliged to prevent malicious cyber activities that originate in their territory.[172] The International Court of Justice (ICJ) has ruled that every state is under the obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states.[173] States thus have a duty of prevention which concerns acts that are unlawful under international law and cause serious physical or other injury on the territory, or to objects, protected by the sovereignty of another state.[174]

Applying this principle to cyberspace, the Tallinn Manual refined ICJs definition arguing that a state shall not allow its cyber infrastructure to be used for unlawful act against other states. This goes for the cyber infrastructure located in the territory of the former state as well as the cyber means under its exclusive governmental control.[175] Hence, the knowledge of such an unlawful act resulting in serious injury is the trigger to act out of 'due diligence' towards other states. However, this 'due dil-

[169] There might have been more military cyber incidents, but these incidents may not have been recognised as such, or incidents were indeed discovered, but not revealed or openly discussed.
[170] Next to the earlier mentioned examples of the military use of cyber weapons in Estonia (2007), Georgia (2008) and Ukraine (2013-2015), military cyber incidents occurred in the Libyan civil war (2011), the Syrian civil war (2013), and the Israel-Hamas crisis (2014). From: Emilio Iasiello, *Are Cyber Weapons Effective Military Tools*?, in *Military and Strategic Affairs*, Volume 7, No. 1, March 2015. Accessed October 16, 2016, http://www.inss.org.il/uploadImages/systemFiles/2_Iasiello.pdf
[171] Emilio Iasiello, *Are Cyber Weapons Effective Military Tools*?, in *Military and Strategic Affairs*, Volume 7, No. 1, March 2015. Accessed October 16, 2016, http://www.inss.org.il/uploadImages/systemFiles/2_Iasiello.pdf
[172] Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in *Peacetime Regime for State Activities in Cyberspace*, edited by Ziolkowski, p 204.
[173] Ibidem.
[174] Ibidem.
[175] Schmitt, *Tallinn manual on the international law applicable to cyber warfare*, Rule 5, p 26.

igence' principle does not mean – by definition – that a state has the absolute obligation to avoid any attack.[176]

The mere fact that knowingly allowing or condoning malicious cyber activities is not authorised under international law does not automatically mean it is not occurring. On various occasions, private and patriotic hacker groups have assumed responsibility for cyber attacks against other states. During the Ukrainian-Russian crisis (2013-2014), the pro-Russian hacker groups 'Quedagh' and 'CyberBerkut' attacked the Ukraine.[177] The latter group also targeted NATO. In both cases obvious Russian state-support seems absent.

The large degree of anonymity, the attribution challenge and the ability of denying knowledge or responsibility all facilitate such practice. In addition, the principle of not knowingly allowing or condoning malicious cyber activities assumes that states are aware and in full control of these activities. With the knowledge that cyberspace is a complex, compiled and diffuse structure, even if there is a (political) will, it is questionable whether states are actually able to supervise and control their part of cyberspace.

2.10.6. Covert operations. The possibility to conduct anonymous operations in cyberspace protects the rights of states as well as enterprises and individuals. Furthermore, anonymous operations facilitate legitimate (e.g., law enforcement) state activities.[178] In addition to noble and legitimate activities, state actors may also operate in a more questionable or clandestine manner (e.g., states could force developers to secretly (re-)design their products to insert particular vulnerabilities or backdoor entries into their hardware or software applications).[179]

Following Snowden's revelations, in 2013, German newspaper 'Der Spiegel' revealed, on the basis of internal NSA documents, that the secret agency exploits technical weaknesses of the IT industry, from Microsoft to Cisco and Huawei.[180] The documents also proved that the NSA intercepts shipping deliveries to plant stealthy backdoor entries in electronics ordered by those it is targeting.[181] Hacker group 'The Shadow Brokers' claims to have hacked the NSA and says to have found sophisticated malware – attributed to the NSA – that manipulates installation scripts, configurations for command and control servers, and that targets specific routers and firewalls.[182] The NSA also appeared to manipulate computer hard drives' firmware with malicious code.[183] These examples may show that actually the entire 'IT-chain' (i.e. hardware, software or protocols) could thus be secretly manipulated at any stage.

From an attacker's point of view one of the advantages of covert operations is that they are unpredictable and invisible to the victim. Once the nature and extent of the effects become clear, the targeted entity can often only assume where the cyber attack came from. An aggressor may further

[176] Robin Geiß and Henning Lahmann, '*Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention',* in *Peacetime Regime for State Activities in Cyberspac*e edited by Ziolkowski, p 655.
[177] Gertjan Boulet, *Cyber Operations by Private Actors in the Ukraine-Russia Conflict: From Cyber War to Cyber Security*, in *American Society of International Law*, Volume 19, Issue 1, January 7, 2015. Accessed October 16, 2016. https://www.asil.org/insights/volume/19/issue/1/cyber-operations-private-actors-ukraine-russia-conflict-cyber-war-cyber.
[178] Ziolkowski, *Peacetime Regime for State Activities in Cyberspace*, p XVI.
[179] Czosseck, *State Actors and their Proxies in Cyberspace*, n 34, p 14.
[180] Spiegel Staff, *Documents Reveal Top NSA Hacking Unit*, in *Spiegel Online International*, December 29, 2013. Accessed October 16, 2016. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html
[181] Ibidem.
[182] Bruce Schneier, *Major NSA/Equation Group Leak*, in *Schneier on Security* blog, August 16, 2016. Accessed October 2016. https://www.schneier.com/blog/archives/2016/08/major_nsaequati.html
[183] Kim Zetter, *NSA's Decade-Long Plan to Undermine Encryption Includes Backdoors, Stolen Keys, Manipulating Standards*, in *Wired Magazine*, May 9, 2013. Accessed October 16, 2016. https://www.wired.com/2013/09/nsa-backdoored-and-stole-keys/

lower its risk of discovery by using a proxy actor to carry out the actual attack. In addition, during the cyber attack the aggressor may exploit the digital identity of a spoofed innocent third party.[184] As attribution is a problem, it is difficult to hold the aggressor accountable for such actions. Covert operations are thus inviting for states that are adversaries.[185]

A mere suspicion of a covert cyber operation of one state into another state's cyber territory would probably affect their mutual relationship, but is not sufficient to execute a retaliatory action. Such a response would require clear traceability and unambiguous attribution.[186] Nevertheless, when capable and willing, the attacked state may respond in equal measure, launching similar covert cyber operations in retaliation. This could lead into escalation of the situation.

The aforementioned DNC email-hack also has the characteristics of a covert (influence / psychological) cyber operation. The hack appears to be an unprecedented attempt to influence the political and electoral process of a nation (the US) by means of a cyber attack.[187] Whether or not this cyber operation is a Russian (state-sponsored) act, this unprecedented activity may be considered as a next step on the cyber-attack escalation ladder.[188] Whoever has conducted this cyber operation, attribution remains a seemingly forensic challenge. Even when full-proof attribution appears to be technically possible, the question is whether that evidence could be published openly, as it would need revelation of the probably also covert and illegal sources and methods of detection. This type of covert action thus provides a high degree of deniability and a limited risk of provoking a strong and quick response.

2.11. International relations. The international relation between states is determined by the foreign policies of states. The previous sections have shown that international laws serve as framework for these international relations. Where appropriate, general principles of international law guide and provide de-confliction for competing sovereign states. In case of a disturbed interstate relationship, diplomacy is a state's primary tool to communicate and negotiate with other states. When diplomacy fails, tougher measures may be taken, such as economic, diplomatic or other sanctions, or the use of force (war). Issues that concern international relations involve, among others, common state interests, underlying values, national security and (armed) conflicts.[189] Choucri states that the introduction of cyberspace has changed the traditional understanding of international relations' conceptual framework (e.g., boundaries, national security, influence, and power politics).[190] Cyberspace appears to disturb the familiar international order.[191]

2.11.1. The influence of cyberspace on international relations. To analyse to what extent cyberspace actually influences international relations the coming section identifies and characterises the interdependencies of two initially separate, yet interconnected domains, namely cyberspace and international relations.

The traditional international system consists of interaction among sovereign states. And traditionally, all other actors were derived from, and legitimised by states. Although the state remains a dominant

[184] Jan Kallberg and Bhavani Thuraisingham, *From Cyber Terrorism to State Actors' Covert Cyber Operations*, ResearchGate, March 2013, Accessed August 2016, DOI: 10.1016/B978-0-12-407191-9.00019-3, Chapter 19, p 232.
[185] Idem, p 231.
[186] Idem, p 232.
[187] Veenendaal et al., *DNC Hack: An Escalation That Cannot Be Ignored*.
[188] Ibidem.
[189] Nazli Choucri, *Cyberpolitics in International Relations*, Massachusetts Institute of Technology 2012, the MIT Press, Cambridge, Massachusetts London, England, 2012, p 3.
[190] Ibidem.
[191] Ibidem.

player in international relations, various types of non-state actors are emerging.[192] Vaishnav, Choucri and Clark mention various changes in international relations, particularly triggered by cyberspace.[193] In short, these changes encompass: (1) whereas at the end of the Cold War the US and the Soviet Union were the main powers, new regional centres of power have emerged and new international organisations play significant roles; (2) traditional hierarchical relations have been replaced by different types of asymmetries and relatively weak hierarchies, if any; (3) there is an expansion of private and public interests, coupled with the creation of new markets and overlapping influences; (4) various types of non-state actors have appeared with various ideological or political agenda's, whereas states are unable to identify their roles, responsibilities or threats; (5) the nature of conflict and war has changed from large-scale war between states to new types of conflict and violence with varying degrees of formal organisation. These changes are isolated events, but together they triggered a paradigm shift as regards the traditional conceptual framework of international relations.[194]

2.11.2. Cyberspace: a new domain of interaction. Vaishnav identifies the ten most important implications of cyberspace as a new domain of interaction. In summary, these changes involve: (1) the dominance of the private sector in an international system;[195] (2) despite new threats to national security, the major actor that constitutes and defines international relations – the state – is unable to control the cyber domain to any meaningful extent; (3) cyber threats to security reinforce the politicisation of cyberspace; (4) the asymmetry in cyberspace[196] may lead to new forms of symmetry;[197] (5) new non-state actors[198] with new interests, new capabilities and new methods to influence lead to new contentions and eventually new potential conflicts; (6) a growing disagreement on the influence and control over the management of cyberspace; (7) various types of cyber conflict facilitate a power shift from historical military dominance to new areas; (8) new forms of international cyber collaboration arise;[199] (9) the cyber-based ability to mobilise civil society across jurisdictions in all parts of the world; (10) An intersection in spheres of influence with the private sector managing order in cyberspace, and sovereign authorities managing order in the physical world.

2.11.3. Contemporary international relations. The two previous paragraphs have shown that governments still play a significant role in relationships with other governments. Nevertheless, non-state actors, such as global and regional inter-governmental organisations,[200] non-governmental organisations, as well as trans-national and multinational corporations, are becoming more influential and have an increasing power in international relations. An example of increasing pressure in international relations and government behaviour was demonstrated in 2014, by Micosoft. No doubt well-intentioned, in an effort to influence the international community, the company published a proposal encompassing six norms for cyber security to limit conflict, "to better define what type of government behaviors in cyberspace" would (not) be acceptable.[201] A multinational company 'dictating' governments how to behave in cyberspace and thus (in)directly influencing international relations.

---

[192] Chintan Vaishnav, Nazli Choucri and David Clark. *Cyber international relations as an integrated system*, in *Environment System & Decisions* (2013) 33: 561–576, Accessed August 20165, DOI 10.1007/s10669-013-9480-3, p 563.
[193] Idem, p 561–576.
[194] Vaishnav (et al.), p. 563.
[195] "Specifically, the Internet is constructed and operated by private sector actors (Internet service providers) located in various legal jurisdictions and minimally regulated in many contexts. The standardization and governance of the Internet is carried out by organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF)", Vaishnav (et al.), p. 563 – 564.
[196] Asymmetry as in "the extent to which weaker actors can influence stronger actors." Vaishnav (et al.), p. 564.
[197] "Such as the ability of a weaker actor to penetrate the computers of stronger actors." Vaishnav (et al.), p. 564.
[198] Such as commercial entities, creators of new markets, proxies for state actors, cyber-criminals, and not-for-profit actors (faith groups, international interest groups, agenda setters, etc.), and the anonymous actors.
[199] Such as a multinational cooperation of Computer Emergency Response Teams (CERT) or the Convention of Cybercrime initiative
[200] Such as the UN, World Trade Organization (WTO), International Monetary Fund (IMF) and European Union (EU).
[201] Angela McKay (et al), *International Cybersecurity Norms Reducing conflict in an Internet-dependent world*, p 11. http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf

As globalisation continues, an inherent conflict in overlapping private and public interests has emerged. Non-state actors, unclear state roles and responsibilities, different interests, concerns and (perceived) threats all influence state matters and decisions in international relations. The aforementioned developments, particularly triggered by cyberspace, have fundamentally changed the way modern international relations are being established and maintained. Consequently, the major actor that establishes international relations – the state – seems unable to control the cyber domain to a meaningful extent. As non-state actors' buy-in will be required for the implementation of worldwide politically binding (cyber) confidence-building measures, this may complicate the development of such measures in general and their implementation in particular.

2.12. Sub-conclusion. Commonly, international laws serve as framework for international relations between states. The perceived absence of cyber-specific laws does not imply that states can enjoy unlimited freedom of action in cyberspace. The duties and responsibilities of competing sovereign states are guided and de-conflicted by three general principles of international law: (1) sovereign equality of states (including four derived principles: self-preservation, territorial sovereignty and jurisdiction, non-intervention, duty not to harm the rights of other states); (2) maintenance of international peace and security; and (3) cooperation and solidarity.

On the basis of these principles, malicious cyber activities could, when they meet the specific UN Charter criteria, be seen as an 'armed attack' or 'use of force' against a state. Such cyber attacks may trigger a self-defence response, escalating into a military conflict and thus threaten international security and stability. States have the obligation to take precautionary measures regarding cyber threats posing a significant international cross-border risk. Coercive interference with domestic or internal state affairs is prohibited. Internet-related cyber-security aspects are considered as of international interest, and fall, therefore, outside of the realm of purely internal affairs. Although all states have a legal obligation to cooperate to reduce cyber activities that threaten international security, the term 'cooperation' is vague and not specified.

On the basis of the sovereignty principle, states (should) have the monopoly on the legitimate use of violence. State actors such as law enforcement, intelligence services, and armed forces act directly on behalf of a state and may conduct operations in cyberspace to exercise (cyber) power and thus use (cyber) violence. For various reasons a state might also use proxy actors, such as cyber criminals, patriotic hackers or other capable non-state actors, working indirectly for that state. From a legal point of view, states may be responsible for direct and indirect cyber operations that their organs conduct on their behalf. Both state actors and proxies generally use the same technologies and methods, however, with differing legitimacy, and for other purposes.

The actual state behaviour that is jeopardising international peace and stability in, though or by cyberspace, encompasses anonymous operations, cyber espionage, the use of proxies, knowingly allowing malicious activities, and the conduct of covert operations. The reasons why these cyber operations can be carried out without virtually any consequences boil down to the large degree of anonymity that cyberspace offers. The attribution problem, in combination with these cyber operations, contributes to interstate distrust, misperception and misunderstanding.

The use of military cyber capabilities for offensive purposes is another type of state behaviour that may endanger international peace and stability. In this case it is not the possibility of anonymous operations that is threatening, but the fact that non-military objects could be targeted; either deliberately or unintentionally. Furthermore, it is hard to distinguish offensive from defensive skills, knowledge or means. Offensive efforts, investments or cyber-weapons are thus easy to deny and easy to hide.

Although the state remains a dominant player in international relations, various types of non-state actors have emerged. New centres of power, weak hierarchies, overlapping private and public interests, non-state actors and unclear state roles, responsibilities and threats, and new types of conflict are influencing traditional international relations. Cyberspace as a new domain of interaction has lead to many changes, including among others, the involvement of the private sector, new threats to national security, asymmetry, power shifts and disagreement on the influence and control over the management of cyberspace. These developments, particularly triggered by cyberspace, have fundamentally changed the way modern international relations are being established and maintained.

As a result, the major actor that establishes international relations – the state – seems unable to control the cyber domain to any meaningful extent. This complicates the development and implementation of worldwide politically binding (cyber) confidence-building measures.

3. Cyber Confidence-Building Measures

Deliberate and focused cyber attacks or cyber warfare constitute a threat to international peace and stability. In the same vein, when misunderstood or misinterpreted, unintentional cyber incidents may escalate into interstate armed conflict.

A common understanding of cyber activities as worldwide threat and a global challenge to international peace and security, has led to the aspiration to develop politically binding confidence-building measures for cyberspace.[202] The previous chapter showed that states have particular duties, responsibilities and authorities. However, states also demonstrate, condone or knowingly allow particular behaviour that may jeopardise cyberspace and, consequently, threaten international peace and stability. The development, acceptance and implementation of cyber confidence-building (CBM) measures may help prevent potential destabilisation and help ensure worldwide confidence in cyberspace. On the basis of existing literature, this chapter provides insight in the various initiatives that have been taken in this area.

To this end, this chapter comprises two main components. The first main section describes what is meant by confidence-building measures and explains the main differences between military and non-military CBM. Thereafter, the recent history of CBM is presented. This section then gives a brief introduction to the UN guidelines for CBM, followed by a more extended view on the work that the organisation for stability and co-operation in Europe (OSCE) is doing in this area. In particular, attention will be paid to the OSCE's 2012 practical 'guide on non-military confidence-building measures', describing *inter alia* the nature, characteristics and limitations of CBM. The first main section ends with an overview of eleven characteristics that successful CBM appear to have in common.

After the first general CBM part, this chapter then focuses on the particular *cyber* confidence-building measures (CCBM). That part subsequently presents an overview of the various recent international, regional and local initiatives to formulate, develop and implement particular cyber CBM. The second section first discusses the preparatory ideas and work of the 'world federation of scientists' information security permanent monitoring panel (PMP)'. Thereafter, the resulting work that has been conducted by the UN group of governmental experts (GGE) since 2010 is presented. Then, the multilateral CCBM-initiatives of the OSCE are considered. Attention is also given to various multilateral, regional and bilateral CCBM-initiatives. This chapter ends with a sub-conclusion.

3.1. A contemporary view on CBM. There is no commonly accepted definition for CBM,[203] however, in general, confidence-building measures (CBM) or confidence and security-building measures (CSBM) are actions taken to reduce the fear of an (armed) attack or the use of force in a situation of tension or conflict. The United Nations office for disarmament affairs (UNODA) defines confidence-building measures as "actions or procedures to prevent hostilities, to avert escalation, to reduce military tension, and to build mutual trust."[204]

The conceptual idea behind CBM is based on positive and negative feedback. The fear or suspicion of a military attack is a 'positive' feedback factor resulting in escalation and, eventually, a conflict.

[202] Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications*, p 11.
[203] OSCE, *Guide on Non-Military Confidence-Building Measures (CBMs)*, Organization for Security and Co-operation in Europe, Vienna, 2012, p 9. Accessed August 2016, http://www.osce.org/cpc/91082?download=true
[204] Military Confidence Building, UN Office for Disarmament Affairs, https://www.un.org/disarmament/convarms/infocbm/

Confidence-building actions or procedures, however, give a 'negative' feedback to the conflict, thereby weakening, cancelling or reversing the tension, and thus preventing escalation into war.[205]

When defining CBM, Mason and Siegfried focus on the negotiating actions that precede the implementation of such measures. They do not particularly focus on the root cause of a conflict.[206] As they mainly focus on the negotiating activities, they use a rather narrow definition.

Ziolkowski paints a wider picture, describing CBM as an instrument of international politics, aiming to prevent the outbreak of an armed conflict resulting from the miscalculation or misperception of the risk of a crisis situation. CBM involve practical measures and processes for inter-state crisis management and usually comprise transparency, cooperation, and stability aspects.[207] Transparency measures aim to foster a better mutual understanding of national military capabilities and activities; cooperation measures include exchange of documents, joint military exercises, exchange of observers, and military delegations visits; stability measures aim to foster predictability of military activities by limitation of these actions, and through the stabilisation of the military balance. Instead of a binding legal commitment, states develop non-binding norms for responsible state behaviour that provides a degree of predictability.[208]

The OSCE identifies two main categories of confidence-building measures: military and non-military CBM.

3.2. Military and non-military CBM. In the modern sense, the military CBM originated from the Cold War and were introduced in 1975 with the adoption of the Helsinki Final Act,[209] by 35 countries,[210] including the two then major opposing military powers: the North Atlantic Treaty Organisation and the Warsaw pact. The parties agreed on ten non-binding principles to guide their mutual relations. Among other things, the participating states came to an understanding to comply with principles such as: sovereign equality; refraining from the threat or use of force; territorial integrity of states; peaceful settlement of disputes; non-intervention in internal affairs; and respect for human rights and fundamental freedoms.[211] In addition to the military CBM that are mainly aimed at limiting the proliferation and use of (conventional) weapons, also various non-military CBM can be identified, such as: political, economic, environmental, societal, or cultural measures.[212] Such non-military measures are closely related to acceptable norms of state behaviour. Both types of measures can be agreed upon multilaterally, bilaterally or unilaterally.

3.3. Stockholm and Vienna documents. Some ten years after the Helsinki Final Act, a follow-up document was adopted: the 1986 'Stockholm document on confidence- and security-building measures and disarmament in Europe'.[213] The document was considered as "the first security agree-

[205] *Confidence and security-building measures. Accessed August 2016*, https://en.wikipedia.org/wiki/Confidence_and_security-building_measures
[206] Simon Mason and Matthias Siegfried, *Confidence Building Measures (CBMs) in Peace Processes* in *Managing Peace Processes: Process related questions. A handbook for AU practitioners*, Volume 1, African Union and the Centre for Humanitarian Dialogue, 2013: 57-77.
[207] Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications*, p 12.
[208] James Andrew Lewis, *Confidence-building and international agreement in cybersecurity*, in *Confronting Cyberconflict*, p 53, UNIDIR Disarmament Forum 4, 2011, Accessed May 4, 2016, https://citizenlab.org/cybernorms2012/Lewis2011.pdf.
[209] OSCE, *Conference on Security Co-operation in Europe: Final Act*, Conference on Security Co-operation, Helsinki, 1975, http://www.osce.org/helsinki-final-act?download=true.
[210] https://history.state.gov/milestones/1969-1976/helsinki.
[211] OSCE, *Conference on Security Co-operation in Europe: Final Act (Helsinki 1975)*, p 4 – 8.
[212] OSCE, *Guide on Non-Military Confidence-Building Measures*, p 9 -11.
[213] OSCE, *Document of the Stockholm Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation in Europe*, Organization for Security and Co-operation in Europe, 19 September 1986. Accessed August 2016, http://hrlibrary.umn.edu/peace/docs/stockholm1986.html.

ment for Europe with significant militarily- and politically-binding, and verifiable CSBMs."[214] It contained mutual complementary confidence- and security-building measures and focused mainly on the practical implementation of these measures, in arranging issues such as prior notification and observation of certain military activities, as well as compliance and adequate forms of verification.[215]

Subsequently, the 1990 Vienna document was adopted, integrating a set of new confidence- and security building measures with the measures earlier adopted in the Stockholm document.[216] Whereas the Stockholm document laid the foundation for various measures, the 1990 Vienna document further specified and consolidated its implementation. The latter document provided *inter alia* detailed arrangements for: the exchange of information on military activities, major weapon systems and military budgets; consultation and co-operation mechanisms concerning hazardous incidents; compliance and verification arrangements; as well as agreements on establishing direct and continuous communications between the capitals.[217]

3.4. UN guidelines for CBM. The UN describes the context, scope, principles, objectives and characteristics of CBM in its 1996 'Report of the Disarmament Commission'. The report reflects, among other things, guidelines for appropriate types of confidence-building measures and for the implementation of such measures on a global or regional level'.[218] These guidelines recognise as: ultimate goal of confidence-building measures "[…] to strengthen international peace and security and to contribute to the prevention of all wars […]."[219] As major objective, the guidelines intend to mitigate the risk of mistrust, fear, misunderstanding and miscalculation resulting from states' military activities.[220] As centrally important task of confidence-building measures, the UN guidelines recognise to enhance security and stability by reducing the dangers of misunderstanding or miscalculation of military activities (e.g., the guidelines help preventing military confrontation and accidental outbreak of wars).[221]

In its description of CBM characteristics, the UN recognises that confidence in international relations is based on political commitments and concrete measures, as well as the belief in the cooperation of other participating states. Confidence and security will increase and tension will lessen when other states show their willingness to exercise non-aggressive and cooperative behaviour. According to the UN guidelines, an essential element of confidence-building is the states' ability to continually verify compliance with agreed provisions. Finally, the UN acknowledges that a detailed universal model of CBM is impractical. Therefore, confidence-building measures must be tailored to a specific situation or region.[222]

On the basis of a survey among 36 member states, a 2011 UN report on 'confidence-building measures in the field of conventional arms'[223] describes that the set of military measures encompass three main categories: (1) information exchange measures; (2) observation and verification

[214] OSCE, *Guide on Non-Military Confidence-Building Measures*, p 12.
[215] OSCE, *Document of the Stockholm Conference*.
[216] OSCE, *Vienna Document 1990 of the Negotiations on Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Vienna Meeting of the Conference on Security and Co-operation in Europe*, Organization for Security and Co-operation in Europe, Vienna, 17 November 1990, p 2. Accessed August 2016, http://www.osce.org/fsc/41245?download=true.
[217] OSCE, *Vienna Document 1990*, p 3 - 48.
[218] UN document A/51/182, *Report of the Disarmament Commission, annex F, the Guidelines for appropriate types of confidence-building measures and for the implementation of such measures on a global or regional level*, 1 July 1996. Accessed August 2016 http://www.un.org/Depts/ddar/discomm/2102.htm#tf.
[219] Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, p 541.
[220] Ibidem.
[221] Ibid.
[222] UN document A/51/182, *Report of the Disarmament Commission, annex F*, para 2.3.
[223] UN document A/66/176, *Information on confidence-building measures in the field of conventional arms*, 25 July 2011.

measures; (3) and military constraint measures. The UN concluded that most of the CBM have been agreed to in regional, sub-regional or bilateral context. Moreover, they reconfirmed that tailoring the measures to the particular security concerns of states within a region or sub-region is crucial.[224]

3.5. OSCE '**Guide on non-military CBM'**. According to the OSCE, classical confidence- and security-building measures (CSBM) refer to specific military issues and are primarily meant to reduce military tensions and the fear of a military surprise attack.[225]

Military confidence-building measures boil down to increasing transparency and predictability, improving information exchange, reducing the risk of misperception and limiting the use of violence by armed forces. The assumption is that exchange of information about military doctrines and resources contributes to stability by enhancing situational awareness and building common understanding. Military CBM or CSBM are valuable as regards the contribution to the de-escalation of an unintended conflict, but are of limited use when conflicts are stimulated intentionally.[226]

According to the OSCE, CSBM are narrower than confidence-building measures and must, therefore, be complemented by non-military CBM in an attempt to involve political leaders and other stakeholders from the wider societies.[227] In their search for a structured manner to develop and implement effective new CBM, the OSCE created a 'Guide on non-military confidence-building measures'.[228]

The guide depicts a conceptual framework that explains, among other things, the nature, characteristics and limitations of CBM. Furthermore, it gives practical guidance on designing and developing new measures. The section hereafter focuses on the OSCE guide, starting with an introductory paragraph about the development and implementation process. Thereafter, the section subsequently discusses the key issues, limitations and obstacles, pitfalls, as well as the necessity of monitoring, verification and guarantees. This section ends with an overview of the eleven characteristics that, in the OSCE's view, successful CBM have in common. The section thereafter focuses on the particular *cyber* CBM initiatives.

3.5.1. Developing and implementing non-military CBM. In the OSCE's view, CBM are usually designed and developed according to a predetermined roadmap. First, a conflict assessment is made. The assessment includes *inter alia* an overview of the main stakeholders and their individual and common interests, as well as potential limiting or obstructive factors. After the initial analysis, an actual 'first move' can be made. The first move could be a (unilateral or multilateral) declaration, proposal, or an invitation to participate in an event, but could also involve the adoption of a decision or a law. Despite the good intention of such a first move, mistrust and fear may complicate the situation. Regarding the development of new CBM the OSCE, therefore, recognised three rules of thumb. As a first rule, they recommend starting with non-controversial issues. The second rule implies that there should be a mutual interest on both sides to engage in dialogue regarding the underlying issues beyond the CBM.[229] The third rule is that areas for co-operation should be built up slowly.[230]

3.5.2. Key issues when creating CBM. In spite of the roadmap, the OSCE guide on non-military CBM does not offer one single or fixed design or result. Therefore, new developments must always

[224] Idem, p 5.
[225] OSCE, *Guide on Non-Military Confidence-Building Measures*, p 14.
[226] Pawlak, *Confidence-Building Measures in Cyberspace: Current Debates and Trends*, in *International Cyber Norms, Legal, Policy & Industry Perspectives*, edited Osula and Rõigas, p 125.
[227] OSCE, *Guide on Non-Military Confidence-Building Measures'*, p 16.
[228] Idem.
[229] OSCE, *Guide on Non-Military Confidence-Building Measures*, p 30.
[230] Ibidem.

be taken into account and new CBM must be tailored to new circumstances.[231] The following issues should be considered when designing new measures.

Depending on the level of tension and mistrust one may commence with symbolic and non-controversial issues that do not cause great risk for either party. Furthermore, appropriate communication channels are required and should be strengthened and extended. Next, in order to find mutual benefit from co-operation, shared values and common interests need to be identified (i.e., in the economic, social or cultural areas). In addition, perceived and real security threats must be taken into account (e.g., the level of criticism persons might receive in their own state). One of the main points to take into account is the various groups that work against effective measures or a solution to the conflict. These spoilers, with a vested power, an economic, or another interest, or merely particular ideologies, may want to frustrate the CBM process (i.e. by provocative actions or by blocking necessary decisions).[232] A final relevant factor is the international environment. The major powers that are in geopolitical and/or economic competition for influence, or other global tensions, could also hamper progress and eventual success.[233] Russia's invasion of the Ukrainian region Crimea in 2014, for example, has disturbed the regional cyber CBM-discussions within the Association of Southeast Asian Nations (ASEAN) Regional Forum.

3.5.3. CBM - limitations and obstacles. Despite their potential to successfully prevent and solve conflicts by improving relationships and behaviour, by their nature CBM also have their limitations. CBM will not change the existing power balances or imbalances and will not eliminate the root causes of a conflict. In their guide on non-military confidence-building measures the OSCE, therefore, also recognises the main factors that limit or obstruct the successful creation of CBM. The three main limitations that may hamper the CBM process are the lack of political will, financial and human resources, or confidence.[234]

A sincere political will to implement CBM is a prerequisite for successful introduction and implementation of CBM. However, the OSCE also acknowledges that in practice opponents may well use the CBM process to just please the international community, whilst trying to obtain unilateral advantage in their best benefit.[235]

In addition, CBM require human and financial resources. A lack of sufficient budget or qualified staff can hamper the development and implementation process. Moreover, if states do not allocate sufficient resources to exchange the required baseline of information, they may also give the wrong signals to other countries. Finally, although CBM intend to increase trust and confidence, at least a minimum level of confidence and readiness to trust other parties is required.

In addition to these limitations, various obstacles may, intentionally or unintentionally, also slow down the CBM process. Groups that are not interested in conflict resolution may frustrate the developments (e.g., security services and political hard-liners, or entities that have otherwise a political or economic interest in continuing the status quo). Furthermore, hard-line declarations by leadership level or the media, policy changes, legal requirements, a weak rule of law and administration of justice, and recurring violence can also hamper progress.[236]

[231] Idem, p 32.
[232] Idem, p 33.
[233] Idem, p 34.
[234] Idem, p 23 – 24.
[235] Idem, p 23.
[236] Idem, p 24 - 25.

3.5.4. Additional pitfalls. Next to the aforementioned limitations, obstacles and key issues concerning the development and implementation of non-military CBM, the OSCE has distinguished various additional pitfalls that should be avoided or addressed in a timely way. These pitfalls include, but are not limited to:[237] (1) A single-level approach, in which either official or only non-official actors are involved. Therefore, extensive interaction is required between all stakeholders (official and non-official actors and various other competing groups from the society (i.e. a 'multitrack diplomacy').[238] (2) Deliberate misuse of CBM. Parties may manipulate CBM to conceal their underlying intentions i.e., to maintain the current situation rather than to solve a particular issue or to merely gain time to strengthen their positions. (3) 'Potemkin CBMs' which are seemingly officially agreed upon, but which are not really implemented or followed-up. (4) Delivery failure. Parties must not promise or imply more than they can deliver. (5) Zero-sum thinking. CBM intend to generate mutual benefits, but may – due to a deep mistrust – be perceived as a zero-sum game in which an advantage to other parties is seen as loss of one's own gain. (6) Misreading. As CBM are often presented as unilateral steps, there is a danger that such CBM are seen as misleading or just an attempt to manipulate the disputed issue in a one-sided way. (7) 'Copy and paste'. As CBM need to be tailored to a specific conflict, good examples and practices from other states or regions must not merely be copied and used in other conflict environments. (8) Politicization. In order to develop successful CBM it is often required to involve non-governmental experts from the civil society who can act independently and who can freely express their opinion. The OSCE also acknowledges that the more political a CBM process becomes, the more difficult it will be for such non-governmental experts to maintain their independent position.[239] (9) Short-cuts. As confidence-building usually is a lengthy process, parties must avoid – in an attempt to accelerate the process – proposing measures that are not really supported by their leadership or society.

3.5.5. Monitoring, verification and guarantees. The political will to follow up and implement agreements is crucial to the eventual success of the measures. Furthermore, sound agreements over definitions, interpretations and steps to be taken are essential principles of a CBM process. However, misinterpretation or disputes on these issues, failure to deliver, or deliberate non-compliance with the agreement are harmful to this process and may thus destroy the carefully built up confidence.[240]

Reliable and trusted information about the progress towards the targets is an essential confidence-building element. Monitoring, verification and guarantee mechanisms can confirm to which extent measures have been implemented and can, when necessary, bring the parties back into compliance with the agreement. These mechanisms thus function as safeguard to all parties. The OSCE, therefore, considers such verification and guarantee mechanisms as 'confidence-building measures in themselves'.[241] The monitoring and verification process may be organised informally, or may be structured more formally on the basis of a clear mandate. The processes can be carried out by the involved parties themselves (as a joint effort, or mutually), by a neutral third party, or through a combination of the parties and a third party.

As regards guarantees two varieties can be distinguished: internal and external guarantees. A legal provision that could only be changed by a super-majority or the consent of all parties is considered as an internal guarantee.[242] The guarantee is thus embedded within the measure itself. External guarantees can be divided into two types: hard or soft. Symbolic promises such as co-signatures or mere

[237] Idem, p 36 – 40.
[238] Multitrack diplomacy is a term for operating on several tracks simultaneously and involves track 1, track 2 (or 1 ½) and track 3 diplomacy (i.e. respectively official-official, official-unofficial and unofficial-unofficial dialogues). From: http://glossary.usip.org/resource/tracks-diplomacy. Accessed October 16, 2016.
[239] OSCE, *Guide on Non-Military Confidence-Building Measures*, p 39.
[240] Idem, p 40 – 42.
[241] Idem, p 41.
[242] Ibidem.

declarations are seen as soft guarantees, whereas legally binding treaties or UN Security Council Resolutions are considered as hard guarantees.

3.5.6. International third parties, such as (impartial) states, international governmental or non-governmental organisations, can play a significant role in the CBM process. These third parties may provide financial, intellectual, political or diplomatic support, or could make available guaranteeing and verification teams.[243] The main challenge is that these parties must maintain an independent and impartial status and not act out of their own agenda.

3.5.7. CBM – Eleven characteristics. As all CBM need to be tailored to a particular conflict, there is no single recipe for successful CBM. Nevertheless, based on their experience with the design, development and implementation of many varying – yet successful – CBM, the OSCE has identified eleven characteristics that these measures have in common:[244]

1	Reciprocity	Although short-term situations may be unequal, the long-term measures, concessions, commitments and advantage must be balanced and mutually acceptable.
2	Incremental	Starting with merely symbolic measures, CBM may be progressively implemented in evolutionary stages of increasing significance.
3	Long-term	Irrespective of any short-term progress or temporary set-backs, CBM need to achieve sustained results on the long run.
4	Predictability	As unpredictable behaviour may trigger unintended responses, the nature, scope and content of CBM should promote parties' predictable behaviour.
5	Transparency	The intent and modalities of a CBM should be obvious, open and unambiguous. There should be no room for misinterpretation of its purposes.
6	Reliability	Proposed CBM need to be realistic, and already initiated CBM need to be carried through. Hence, CBM need to be reliable.
7	Consistency	CBM should be consistent with regard to topics, messages or target groups. Inconsistency will eventually lead to mistrust that undermines the entire CBM process.
8	Communication	Appropriate communication channels are required to provide for direct dialogue to clarify potential misunderstandings, misperceptions or mistakes.
9	Verification	Particularly in cases where reciprocity is expected, verification (possibly by third parties) is an important component in reducing parties' fear and mistrust.
10	Local ownership	The successful long-term implementation of CBM depends on the voluntary engagement and real commitment of all parties. To that extent the interests, concerns, needs and priorities of all relevant parties must be taken into account.
11	Multi-level	CBM can be developed top-down or bottom-up, but involvement of both government structures and civil society at large is an essential prerequisite for lasting success.

Figure 1: OSCE's characteristics of successful CBM

3.6. Cyber CBM initiatives. Ziolkowski argues that many states already acknowledge the possibility that malicious cyber activities could result in an armed military conflict, even if this would be the

[243] Idem, p 46.
[244] Idem, p 16 – 19.

result of a misperception or miscalculation of the perceived risk.[245] Traditional CBM should lead to an adequate level of predictable international state behaviour that, in its turn, reduces the chances of losing control during crisis situations. According to Ziolkowski, the ultimate end-state of cyber CBM would encompass a worldwide understanding of acceptable state behaviour and cyber stability in international relations.[246] Cyber confidence-building measures should thus help prevent military conflicts. The coming section describes how, in the past few years, the CBM development and implementation process has been applied to cyberspace.

3.7. Information Security Permanent Monitoring Panel. One of the first initiatives that related confidence-building measures to cyber came from the World Federation of Scientists. According to their information security Permanent Monitoring Panel (PMP),[247] a comprehensive legal framework to manage and control the rapidly evolving cyberspace does not yet exist. As a consequence, there are no means to effectively manage any escalations in a cyber conflict either. Moreover, even a commonly shared interpretation of how the existing international laws should apply to cyberspace, is yet lacking.[248] The PMP recognized that offensive cyber capabilities constitute yet another potential threat to national and international peace and security. Furthermore, the PMP acknowledged that some states have developed high-tech capabilities that can be used to launch cyber attacks on, for example, other states' critical infrastructures. Such cyber attacks may not only harm the infrastructure, but also severely jeopardise the national security of the attacked state.[249]

As from its inauguration in 2001, the PMP, therefore, aims at creating a universal order of cyberspace and controlling cyber conflict. To achieve that goal, they recommended a comprehensive legal framework, as well as norms and rules for responsible state behaviour.[250]

3.7.1. Unified effort required. In 2003, in its first publication, the information security PMP acknowledged the global nature of cyberspace, and the trans-national character of cyber security challenges for society, states, and individuals. The PMP advocated the peaceful use of cyber space, but realised that this challenge could not be resolved by the efforts of just one state or a group of states, or on a regional basis. They came to the conclusion that the solution to this problem would require a unified effort of the entire international community.[251]

3.7.2. Leading role for the UN. The PMP issued thirteen recommendations, mainly stemming from the idea that the UN should play the leading role in engaging international activities relative to the functioning and protection of cyberspace, to reduce the ability that cyberspace is exploited for malicious and aggressive purposes.[252] The UN should particularly concentrate on a comprehensive Law of Cyberspace, the harmonisation of national cyber-crime laws and procedures for international co-operation and mutual assistance.[253]

---

[245] Ziolkowski, *Confidence Building Measure for Cyberspace*, in *Peacetime Regime for State Activities in Cyberspace*, p 533.
[246] Idem, p 13.
[247] The World Federation of Scientists Information Security Permanent Monitoring Panel (PMP) was established in 2001, in order to examine the emerging threat to the functioning of information and communication technology (ICT) systems and to make appropriate recommendations, from: http://www.federationofscientists.org/
[248] Henning Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, in *International Seminar on Nuclear War and Planetary Emergencies*, edited by Richard Ragaini, 45th Session: The Role of Science in the Third Millennium, Singapore: World Scientific Publishing Company, 2013, p 457
[249] Henning Wegener et al., *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report and Recommendations, p 11, World Summit on Information Society, Geneva 2003 – Tunis 2005, Document WSIS-03/GENEVA/CONTR/6-E 19 November 2003.
[250] Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, p 457.
[251] Wegener et al., *Toward a Universal Order of Cyberspace*, p 14 - 15.
[252] Idem, p 15 - 17.
[253] Idem, p 18.

3.7.3. Cyber treaty unfeasible. The Panel initially envisaged a 'Convention on Cyber Space', comparable to the 'UN Convention on the Law of the Sea of 1982', but also acknowledged that developing such an instrument would entail great difficulties.[254] Both the universal treaty-making and the national ratification procedures would be lengthy processes, disproportionate to the urgency to fill the existing legal gaps. Such a lengthy process would not reflect the worldwide view of the already existing and sharply rising threat of cyber warfare and the resulting uncontrollable damage.[255] The PMP came to the conclusion that legally binding commitments to avoid cyber attacks and corresponding sanctions were, although preferred, unfeasible. Rather than focussing on treaties, they instead decided to concentrate on regulating behaviour though (1) confidence-building measures and (2) codes of conduct as normative tools.[256]

3.7.4. A window of opportunity for CBM. In the view of the PMP, confidence-building measures open a window of opportunity as such measures could enhance transparency and make state behaviour more predictable and, as a consequence, reduce threat.[257] In addition, the Panel argues that CBM offer the possibility to include both state and non-state actors, and also allow participants to independently adopt and enact partial solutions. Besides, whereas treaties are legally binding, CBM are – at most – politically binding and, therefore, better suited to stimulate international consensus-building.[258]

3.8. Worldwide CCBM-initiative - UN Group of Governmental Experts. In line with PMPs suggestion that the UN should have a leading role in inter-governmental activities for the functioning and protection of cyberspace, in 2009, the UN established a Group of Governmental Experts (UN GGE)[259]. The Group consisted of experts from, among others, Brazil, China, India, the Russian Federation and the United States of America.[260] One of their goals was to recommend feasible measures to achieve international cooperation in order to enhance worldwide cyber security.[261]

The UN GGE acknowledged that various international efforts had been conducted to combat cybercrime, particularly within "the Shanghai Cooperation Organization, the Organization of American States, the Asia-Pacific Economic Cooperation Forum, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Economic Community of West African States, the African Union, the European Union, the Organization for Security and Cooperation in Europe and the Council of Europe, as well as through bilateral efforts between States."[262]

However, the Group recognised that other, non-criminal areas of trans-national concern should also receive appropriate attention. These concerns include the lack of international norms for state behaviour in cyberspace and the consequent risk of misperception and potential escalation in cases of major cyber incidents.[263] This risk would argue for the introduction of cooperative actions and mecha-

[254] Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, p 457.
[255] Idem, p 458.
[256] Ibidem.
[257] Ibid.
[258] Idem, p 458 - 459.
[259] i.e. the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security'.
[260] The UN Group of Experts was established pursuant to paragraph 4 of the UN General Assembly resolution 60/45. In accordance with the terms of the resolution, experts were appointed from 15 States: Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland and the United States of America.; from: http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf
[261] UN document A/65/201, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 30 July 2010, p 6.
[262] Idem, p 7.
[263] Ibidem.

nisms, and underlines the urgent need for international multi-stakeholder collaboration to enhance transparency and stability, build confidence, reduce lurking risks and eventually manage incidents.[264]

3.8.1. The first UN GGE attempt. In their first (2010) report the UN GGE recommended five actions for the development of confidence-building and other measures to reduce the risk of misperception resulting from cyber disruptions. Next to the recommendation to develop common terms and definitions and to support capacity-building in support of less cyber-developed countries, the UN GGE advocated to discuss norms pertaining to state use of ICT. Furthermore, the Group suggested the development of confidence-building, stability and risk reduction measures, including exchanges of national views on the use of ICT in conflict. Finally, the UN GGE proposed information exchanges on national legislation and national ICT security strategies and technologies, policies and best practices.[265] According to Tikk-Ringas, the UN GGE failed to adopt a consensus report partly due to considerable differences on views.[266]

3.8.2. UN GGE 2015 report. Since 2010, the UN GGE issued annual reports on this very topic. In their latest consensus report the UN GGE (2015)[267] observes a significantly increase in cyber incidents stemming from the malicious use of cyber capabilities by state and non-state actors.[268] As existing and emerging threats they also recognise, among other things, the development of cyber capabilities for military purposes, the diversity of malicious non-state actors and the difficulty of attribution.[269] The UN clearly acknowledges the risks that cyber attacks pose to international peace and stability.

The GGE recommends a set of voluntary, non-binding norms for responsible state behaviour that do not only specify what a state may, or may not do in cyberspace. Moreover, the norms describe which activities, executed by non-state actors, should be not knowingly allowed or condoned either.[270] A significant area of attention is the protection of critical infrastructures (CI). States should refrain from cyber attacks on CI, and have the obligation to appropriately protect their own CI against cyber attacks.[271] The former is remarkable – the report does *not* limit these norms to peacetime – as the UN thus proposes to exclude objects from *cyber* attack, while these objects are not otherwise excluded from traditional *kinetic* military attack. This would mean that attacking and permanently destroying Critical Infrastructure with bombs is allowed, whereas a temporary shutdown by cyber means would constitute a violation of the norms for responsible state behaviour.

In a similar vein, states' Computer Emergency Response Teams (CERT) should also be considered as out of bounds for cyber attacks. Furthermore, the GGE 2015 recommends a set of voluntary (cyber) CBM, mainly encompassing the usual information exchange, cooperation and transparency aspects.[272] Both Russia and China agreed on the voluntary norms that were initially introduced at the

[264] Ibidem.
[265] UN document A/65/201, p 8.
[266] Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, Ict4Peace Cyber Policy Process Brief, p 7. http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf
[267] The UN Group of Experts 2015 included experts from 20 States: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Republic of Korea, Russian Federation, Spain, United Kingdom of Great Britain and Northern Ireland, United States of America. From: UN document A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015.
[268] Idem, p 6.
[269] Ibidem.
[270] UN document A/70/174, p 7 – 8.
[271] Idem, p 8.
[272] Idem, p 9 – 10.

request of the US. This is notable as from the first two states' perspective these voluntary norms could be the prelude to (unwanted) *legally binding* norms.[273] Nevertheless, they agreed.

The UN GGE reiterated their 2013 landmark observation that the international law, and in particular the Charter of the UN, is applicable to cyberspace.[274] A key element in their 2015 report is the elaboration on *how* international law should be applied. The proposals touch upon, among other things, jurisdiction over cyber means within a territory;[275] the use of proxy actors; the 'due diligence' principle;[276] and the substantiation of accusations that states are involved in cross-border cyber attacks.[277] Despite the attention paid to the issue, in the opinion of the US and other Western states, the paragraphs specifying *how* law applies to cyberspace are still considered being insufficiently robust.[278]

In view of the size and composition of the GGE, the variety of controversial issues and the consequent diverging opinions, it is noteworthy that the Group managed to reach a diplomatic consensus at all.[279] The UN GGE has proven to be workable and, to a certain extent, successful. However, the amount of participants thus far ranged from fifteen to twenty – yet influential – UN member states. To ensure legitimacy and acceptance, a bigger audience needs to be involved in future negotiations.[280] [281]To that extent, in line with their earlier position that confidence-building measures should be tailored to a situation and region,[282] important ground-work may be carried out by smaller, regional committees. Nevertheless, eventually the UN as a whole needs to come to a multilateral, comprehensive result. Given the sensitivity of the topics, the diverging opinions, and the potential amount of UN member states involved (193)[283] this may be a long and difficult process.

3.9. Multilateral CCBM-initiative - OSCE. In December 2013, the organisation for security and co-operation in Europe (OSCE),[284] adopted an initial set of eleven (cyber-related) CBM in an effort to address cyber security.[285] The OSCE measures would complement the UN efforts to promote cyber CBM. The OSCE decision is primarily based on voluntary and practical risk-reduction measures. In order to enhance transparency and reduce misperception and escalation between states, the measures focus mainly on information sharing and cooperation at the government- and expert-level. Furthermore, with the intent to enhance international cooperation and stability, the measures include the use of the OSCE as an ideal forum for exchanging best practices.[286] Given their experience in confidence-building between opposing forces during the Cold War, this platform seems a feasible start. However, large parts of the world would still not be involved in the process.

---

[273] Henry Rõigas and Tomáš Minárik, *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, in *Incyder News*, August, 2015. Accessed October 18, 2016, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.
[274] UN document A/70/174, p 12 art 24.
[275] Idem, p 12 art. 27a.
[276] Idem, p 13 art. 28e.
[277] Ibidem.
[278] Elaine Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?* in *Lawfare*, September 12, 2015. Accessed October 18, 2016. https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.
[279] Ibidem.
[280] Ibidem.
[281] The fifth UN GGE (2016/2017) involves 25 UN Member States, including the Netherlands.
[282] UN document A/51/182, *Report of the Disarmament Commission, annex F*, para 2.3.
[283] There are 193 UN Member States that are also member of the UN General Assembly. From: http://www.un.org/en/member-states/ Accessed October 21, 2016.
[284] The OSCE has 57 participating States from Europe, Central Asia and North America; from: http://www.osce.org/States
[285] OSCE, *Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1106 (Organization for Security and Co-operation in Europe, Permanent Council, 975th Plenary Meeting, 3 December 2013, p 1.
[286] *Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna*, 7 November 2014, Accessed August 2016, http://www.osce.org/cio/126475

In exchange for their support to this OSCE CBM, in an attachment to the document, the Russian Federation demanded a commitment to respect the principle of non-interference in internal state affairs,[287] as well as the sovereign right of states to govern the internet in their national part of cyberspace.[288] With this annex, Russia reiterated their 2011 code of conduct's main viewpoint regarding international norms and rules for state behaviour in 'the information space': the right to sovereignty, territorial integrity and political independence for all states.

3.9.1. OSCE second set of CBM. Almost one year later, in November 2014, a broad range of specialists and professionals discussed the implementation of the confidence-building measures, while exploring the development of a second set of additional CBM. That second set of CBM was adopted in March 2016, and again primarily based on voluntary commitments, information exchange, co-operation and transparency.[289] The second group of confidence-building measures builds further on the initial set of CBM, but contains also five additional measures that boil down to the following.[290]

Interstate exchanges on the regional and/or sub-regional level in different formats are recommended. These meetings may further investigate the spectrum of co-operative measures, processes and mechanisms. Participation of the private sector, academia, centres of excellence and civil society in such activities is encouraged. Another measure involves the establishment of specific ICT-related communication channels to prevent and reduce the risks of misperception, escalation, and conflict. Furthermore, the formation of public-private partnerships to respond to common security challenges is advocated.

3.9.1.1. Securing critical infrastructures. One of the OSCE's measures is specifically dedicated to securing critical infrastructures and the national and trans-border ICT networks upon which such critical infrastructures rely. The final additional measure involves responsible reporting of vulnerabilities to businesses and industry, and their potentially available remedies. In addition to the additional set of measures, the OSCE also decided that participating states will meet regularly, at the level of designated national experts, to discuss the information exchanged and to explore the appropriate development of CBM.[291]

3.9.2. OSCE Informal Working Group. A recently held OSCE Informal Working Group (October 2016) showed that the process, after a successful start, has now nearly come to a standstill. The implementation of the earlier agreed CBM is delayed by various internal disagreements and accusations of state (sponsored) hacking activities. This event illustrates that geopolitical competition and tensions between the world powers may indeed have a negative impact on the cyber CBM discussions. The way forward for the OSCE Working Group appears to be unclear.[292]

3.10. Regional CCBM-initiative - Shanghai Cooperation Organisation. Already in 2001, the Russian-Chinese led Shanghai Cooperation Organisation (SCO)[293] sent a draft proposal for a code of

[287] OSCE, *Decision No 1106, Interpretative Statement Under paragraph IV.1(A)6 of the rules of procedure of the Organization for Security and Co-operation in Europe*, Attachment, p 4.
[288] Ibidem.
[289] OSCE, *Decision No 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1202, Organization for Security and Co-operation in Europe, Permanent Council, 1092nd Plenary Meeting, 10 March 2016.
[290] Idem, p 3 – 5.
[291] Idem, p 4 – 5.
[292] 'OSCE Informal Working Group Established by PC Decision 1039', Informal Working Group on Cyber CBMs report of the meeting that took place on October 11, 2016. The report is classified, and is - upon request - accessible via the author.
[293] The Shanghai Cooperation Organisation is a Eurasian political, economic, and military organisation which was founded in 2001 in Shanghai by the leaders of the People's Republic of China, Kazakhstan, Kyrgyz republic, the Russian Federation, Tajikistan and Uzbekistan. Accessed August 2016, 'what is SCO', http://infoshos.ru/en/?id=51

conduct to the UN with the intent to define internationally acceptable norms and rules for state behaviour in cyberspace.[294]

3.10.1. Code of conduct. The draft code of conduct (CoC) expressed, *inter alia*, the right to sovereignty, territorial integrity and political independence for all states, and proposed not to use ICT for hostile activities or to pose threats to international peace and stability. Furthermore, the code of conduct envisaged the establishment of a multilateral, international internet management system, and advocated an important role for the United Nations in formulating international norms. Adherence to the code would be on a voluntary basis and open to all states.[295]

3.10.2. Western opposition. Many Western governments opposed the CoC for multiple reasons. They interpreted the code as a threat to the existing free flow of information.[296] In addition, they saw the proposal as a steppingstone towards a legally binding treaty, trying to regulate state activities in cyberspace, whereas Western governments would mainly prefer to apply existing international law or politically binding norms. Ironically, whereas Western states wanted to stay away from legally binding issues in the code of conduct, Russia and China were afraid of legally binding topics in the UN GGE 2015 report. It should be noted, however, that although the proposed CoC comprises norms, these norms are non-binding and of a voluntary or ambitious nature.[297] Another issue and reason for Western resistance was the prospect to change the internet governance. As alternative for the traditional US-dominated internet governance, the CoC promoted a broader, multilateral internet management system.[298] Eventually, the draft proposal was not put to the vote.[299]

3.11. Multilateral CCBM-initiative – ASEAN regional forum. The association of Southeast Asian nations (ASEAN) regional forum (ARF) is one of the main forums for the discussion of cyber CBM in Asia. The ARF brings together the ten ASEAN members, seven other regional states and the ten ASEAN dialogue partners, including the US, Russia, China and the European Union.[300] The ARF discusses political and security issues and intends to make significant contributions to preventive diplomacy and confidence-building measures. Since 2012, ARF focuses also on cyber security.

With their 2015 work plan the ARF intends to develop, among other things, trust and confidence between the various states in the region. In addition, they aim to create an open and secure cyber environment within which states cooperate. This should facilitate the prevention of conflict and crisis.[301] One of the work plan's concrete objectives is to promote transparency and develop CBM. This should reduce the risk of misperception and miscalculation and should prevent the escalation of cyber incidents into an actual conflict.[302] The other objectives aim at cyber security threat awareness; co-operation to protect ICT-enabled critical infrastructures; and regional capacity to respond to criminal and terrorist use of cyber means.[303]

---

[294] UN document A/66/359, *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*, 14 September 2011, p 4.
[295] Idem, p 4 – 5.
[296] Osula and Rõigas, *International Cyber Norms, Legal, Policy & Industry Perspectives*, p 18.
[297] Ibidem.
[298] Ibidem.
[299] Idem, p 17.
[300] Pawlak, *Confidence-Building Measures in Cyberspace: Current Debates and Trends*, in *International Cyber Norms, Legal, Policy & Industry Perspectives*, edited by Osula and Rõigas, p 141.
[301] ASEAN Regional Forum *Work Plan on security of and in the use of information and communications technologies (ICTs)*, 7 May 2015, Accessed August 2016: http://aseanregionalforum. asean.org/files/library/Plan%20of%20Action %20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf.
[302] ASEAN Regional Forum *Work Plan*, p 1.
[303] Ibidem.

The 2015 work plan contains proposals for two main activities, of which the first one is to form a study group that focuses on the development of CBM aimed at reducing the risk of cyber incidents escalating into conflicts.[304] The study group should, among other things, develop processes and procedures for information sharing, and recommend confidence-building measures. The second main activity concerns the conduct of workshops and seminars to assess the possibilities regarding, among other things: information sharing; co-operation; incident prevention; capacity-building; developing norms, rules and principles for responsible state behaviour; raising awareness; and unambiguous terminology.

The ARF's intentions and goals and objectives are in line with the UN. As Pawlak notes, the measures that ARF proposes are also quite similar to the OSCE's set of CBM.[305] He also notes that compromises within the Forum are difficult to find, due to the complicated relations between the various actors (e.g., in addition to the ASEAN members, among others, also the US, Russia, China and the EU), different political systems, and levels of development. Furthermore, Pawlak concludes that the OSCE's progress to date in the CBM development process could be very helpful in developing measures that the various ARF states are probably willing to accept.[306] The diverging intentions and different goals of the individual states within the ARF,[307] the discussions and the poor results thus far may characterise a foretaste of future, worldwide discussions.

3.12. Regional CCBM-initiative – OAS. The organisation of American states (OAS), an intercontinental organisation aiming at regional solidarity and cooperation among its 35 independent American member states,[308] followed a different approach. Already in 2004, the OAS adopted a strategy to combat threats to cyber security. On the basis of a joint fight against terrorism, the member states agreed to develop 'a culture of cyber security in the Americas' by taking the necessary measures to prevent and respond to cyber attacks.[309] In 2012, the OAS reiterated its anti-terrorism position with a cyber security declaration that mainly reaffirmed and strengthened their earlier statements.[310] This declaration was followed by yet another declaration in 2015.[311]

Although not labelled as such, the OAS cyber security strategy and subsequent declarations contain various confidence-building measures, with the main objective to be able to quickly and adequately respond in cases of cyber security threats, incidents and crises.[312] The initial strategy focuses on concrete cooperation measures, exchange of information and capacity building.[313] The 2012 declaration builds further on the same aspects, but with a specific view on fighting cyber terrorism. This shift has given an additional impetus to cooperation. In 2015, the scope was broadened to particularly include the critical infrastructures.

---

[304] Ibidem.
[305] Pawlak, *Confidence-Building Measures in Cyberspace: Current Debates and Trends*, in *International Cyber Norms, Legal, Policy & Industry Perspectives'*, edited by osula and Rõigas, p 144.
[306] Ibidem.
[307] e.g., differing positions on state control over the internet and its content versus freedom of speech; privacy; censorship.
[308] http://www.oas.org/en/about/who_we_are.asp
[309] OAS, *Adoption of a comprehensive inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinair approach to creating a culture of cybersecurity*, AG/RES. 2004 (STATEIV-O/04), 8 juni 2004, Accessed August 2016, http://www.oas.org/STATEIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cy-bersecurity.htm.
[310] Inter-American Committee Against Terrorism (CICTE), *Declaration: Strengthening Cyber-Security in the Americas*, March 9, 2012. Accessed October 18, 2016, http://www.state.gov/p/wha/rls/221498.htm
[311] Inter-American Committee Against Terrorism (CICTE), *Declaration Protection of Critical Infrastructure From Emerging Threats*, March 23, 2015, Accessed October 18, 2016, https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf
[312] OAS, *Adoption of a comprehensive inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinair approach to creating a culture of cybersecurity*.
[312] Idem, Appendix A, Appendix 1.
[313] Ibidem.

The US dominance over the internet and its political and economic influence in the region are obvious and significantly determine the outcome of any negotiation involving cyber in the region. In contrast to the ARF, the relations between the various OAS states seem far less complicated while the different political systems are less extreme. The seemingly united stance and determination of the OAS to combat cyber terrorism resulted in a cyber security strategy and subsequent declarations that mainly encompass cooperative, information exchange and capacity building measures. Yet, the usual CBM-related transparency measures are conspicuously absent. Worthy of note is also that the organisation keeps urging member states to agree, sign, ratify and implement the various declarations.[314] This could be an indication that, although states are willing to consent politically, the implementation of the various measures in practice, may appear to be more difficult. Whether this lacking implementation is occurring for reasons of political unwillingness or for merely practical reasons, is yet unclear. In the latter case, capacity building may be a helpful instrument.

3.13. Bilateral CCBM-initiatives. Alongside the UN, OSCE, SCO, ARF and OAS initiatives, the three major cyber power blocks US, Russia and China have also made bilateral agreements, either in the form of a formal treaty or a more informal politically binding arrangement. As is the case with many global issues, a constructive US-Russian-Chinese relationship with regard to cyber CBM is also a condition for success. A disturbed relationship between these major powers will likely also stall the CCBM process for others.

In 2013, the US and Russia announced a bilateral agreement concerning the cooperation on ICT security. Through extensive transparency and confidence-building measures the two powers aim to reduce the mutual danger they are facing from cyber threats. These CBM supplement an earlier document on this issue. Both powers want to realise threat reduction by strengthening their relations in cyberspace, and by taking confidence-building measures. In particular, they want to expand their mutual understanding of cyber threats that appear to originate from each other's territory. Furthermore, they aim at preventing the unnecessary escalation of cyber security incidents.[315] To mitigate the cyber security risks to critical systems, the exchange of practical and technical information between the US-CERT and its Russian counterpart has been agreed upon. Furthermore, both states decided to use the already existing 'nuclear risk reduction centre' (NRRC) communication links as 'hotline' to manage crisis situations and to reduce the possibility of misperception and escalation from ICT security incidents of national concern.[316] However, the crisis in Ukraine and the Russian annexation of Crimea have impeded this development. In 2014, in a report on US-Russia relations, the US International Security Advisory Board recommended that instead of finding ways to improve the relationship, the United States must now focus on a more confrontational relationship.[317]

In 2015, Russia and China made a bilateral cyber security deal involving two main aspects: 'non-aggression in cyberspace' and 'cyber-sovereignty'. The pact mainly builds further on the earlier mentioned (Russian-Chinese led) Shanghai cooperation organisation's code of conduct. However, the non-aggression pledge is new. Whereas the non-aggression part is mainly about limiting mutual cyber-espionage, the cyber-sovereignty element has a much wider political and strategic objective.

[314] CICTE *Declaration Protection of Critical Infrastructure From Emerging Threats*, Art 2, p - 6
[315] White House, the. Office of the Press Secretary. *Factsheet US-Russian agreement on cooperation on information and communications technology security*, 17 June 2013. Accessed August 2016, https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.
[316] Ibidem
[317] US Department of State International Security Advisory Board, *Final Report of the International Security Advisory Board (ISAB) on U.S.-Russia Relations*, December 9, 2014, p 3. http://www.state.gov/documents/organization/235118.pdf

Yuxi Wei explains that Russia and China have a shared strategic interest in laying down rules for 'cyber-sovereignty'. This view contradicts the US plea for worldwide 'cyber-freedom'.[318]

Russia and China both consider the internet as a state's sovereign territory, within which state control over domestic cyberspace is justified, and without any foreign interference. Furthermore, Wei observes that both states do not commit themselves to reducing mutual cyber-espionage or enhancing trust. Rather, their cyber security deal appears to aim to erode the US dominance over the internet.[319] Wei concludes that the strengthened bilateral ties between China and Russia are motivated by their joint fear for and the opposition to US dominance over the internet, rather than the aim to forge a real cyber alliance. Their cooperation reflects their determination to reshape international politics and cyber security norms.[320]

Also in 2015, the US and China agreed to expand and deepen their bilateral cooperation in, among other topics, the cyber security area. One of the drivers for the agreement was the US-desire to reduce China's economically-motivated cyber espionage.[321] The agreement entails, among other things, to refrain from the conduct or knowingly support of cyber-enabled theft of intellectual property, trade secrets or other confidential business information. Furthermore, both states agree to make a common effort to further identify and promote appropriate norms of state behaviour in cyberspace within the international community.[322] Other arrangements or what the US promised in return, remains unknown as the deal has not been published.

One year on, FireEye's[323] tentative conclusion is that Chinese economic cyber espionage has indeed been drastically reduced in the past two years.[324] China thus seems to abide its pledge not to hack American trade secrets or intellectual property. However, the situation is complicated. Both states agreed not to conduct *economic* cyber espionage. Political, diplomatic, (national) security related or other cyber espionage activities were not explicitly excluded and are, therefore, implicitly still tolerated. This would still allow the hacking of governmental organisations, commercial businesses or virtually any other entity for reasons of, for example, national security; by both states. Illegally copying an adversary's military billion dollar project for reasons of national security would thus be acceptable, whereas the same activity would be unacceptable if carried out for other reasons. The dividing line between commercial and other types of (cyber) espionage thus remains blurred; or rather, it is the – sometimes unclear – actual intent behind the espionage that blurs this matter.

Despite the optimism about the perceived reduction in hacking activities, it is premature to conclude that China has permanently ceased its state or state-sponsored cyber economic espionage activities in the US. Perhaps China just wants to lie low for a while, as they are too embarrassed by the revelation of their (commercial) cyber espionage activities and the resulting charges the US filed against five

[318] Yuxi Wei, *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty*, Jackson School of International Studies, University of Washington, June 21, 2016, Accessed August 2016, https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/.
[319] Ibidem.
[320] Ibidem.
[321] Warren Harold, Scott, *The US-China Cyber Agreement, a good first step*, RAND corporation, August 1, 2016. Accessed August 2016, http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.
[322] White House, the, Office of the Press Secretary. *Fact sheet 'President Xi Jinping's State Visit to the United States*, September 25, 2015. Accessed August 2016, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States.
[323] FireEye is the US Cyber security company known for blaming a specific unit of China's Peoples Liberation Army for a major campaign of economic espionage in 2013; http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D
[324] Reuters World News, *Chinese economic cyber-espionage plummets in U.S.: Experts*, June 21, 2016. Accessed October 2016, http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D

Chinese military hackers.[325] This temporary 'lull in the battle' would then allow China to develop even more sophisticated and stealthier cyber tools and techniques to remain undetected in future attempts.

3.14. Other initiatives. Apart from the aforementioned initiatives some more projects have been launched in the search for cyber CBM. In recent years, various subsequent international cyber conferences were held, with confidence-building measures as one of the major topics (e.g., London, Berlin, Beijing, Vienna, Budapest, Seoul, and The Hague).[326] In addition, the Asia-Pacific Economic Cooperation (APEC), the Shanghai Council and the Council of Europe, Non-Governmental Organisations (NGO) in the cyber area and individual scientists are working on the development of CBM arrangements or cyber Codes of Conduct.[327]

The various global, regional, local and bilateral initiatives show that concluding agreements is possible. However, the limited scopes and poor results also reveal that there is a yawning chasm between idealism and pragmatism; as is the case in other global fields. Although such diplomatic efforts fit in the wider strategic frameworks to develop stability, the agreements that major powers conclude often create the appearance of pragmatism: norms and measures are seemingly intended to preserve one's own freedom of action in cyberspace, whilst strictly demarcating the margins left to others. The fact that these arrangements have not been publicly released does not engender great trust.

3.15. Sub-conclusion. Malicious cyber activities carry the risk of misperception and unintended escalation into a military conflict and thus threaten the international security and stability. Confidence building measures (CBM) are the pre-eminent instrument of international politics to prevent the outbreak of interstate armed conflicts. CBM do not focus on the root causes of conflicts and do not involve legally binding commitments. Instead, by establishing non legally-binding norms for responsible state behaviour in the form of practical measures and processes, CBM aspire to build mutual trust and aim to enhance security and stability. Furthermore, they aim to provide a degree of international predictability. These measures usually contain aspects of transparency, cooperation and stability. The ultimate *cyber* CBM would include a common understanding of responsible state behaviour in cyberspace and a state of cyber stability in international relations.

In its description of CBM characteristics, the UN recognises that confidence in international relations is based on political commitments, concrete measures and the belief in cooperative and non-aggressive behaviour of other states. A crucial element of confidence-building is the states' ability to continually verify compliance with agreed provisions. The UN acknowledges that a detailed universal model of CBM is impractical. Consequently, CBM must be tailored to a specific situation or region.

Whereas military CBM are mainly aimed at limiting the proliferation and use of weapons, non-military CBM are closely related to acceptable norms of state behaviour. Both types of measures can be agreed upon multilaterally, bilaterally or unilaterally. In the view of the OSCE, military CBM are valuable as regards the contribution to the de-escalation of an unintended conflict, but are of limited use when conflicts are stimulated intentionally. In its 'Guide on non-military confidence-building measures', the OSCE depicts a conceptual framework that gives practical guidance on designing and developing new CBM. The guide underlines the need to thoroughly assess the conflict and to map

[325] US Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, Mat 19, 2014. Accessed October 19, 2016, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
[326] Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, in *International Seminar on Nuclear War and Planetary Emergencies*, edited by Richard Ragaini, p 459.
[327] Idem, p 459 – 460.

the main stakeholders and the potential spoilers (i.e. the various groups that work against effective measures or a solution to the conflict). The guide identifies a wide range of limitations, obstacles and other pitfalls that may complicate the development of successful CBM. Finally, the guide stresses the necessity of monitoring, verification and guarantees.

One of the first initiatives that related CBM to cyber came from the World Federation of Scientists information security Permanent Monitoring Panel (PMP). The PMP advocated an international approach and envisaged a leading role for the UN. The Panel realised that a universal legally binding treaty would not be feasible and instead recommended to concentrate on regulating behaviour though politically binding confidence-building measures. CBM would offer the possibility to include both state and non-state actors, and also allow participants to independently adopt and enact partial solutions.

The UN took up the challenge and since 2010 the UN Group of Governmental Experts (GGE) issued annual reports on this topic. In their latest (2015) report the GGE observes a dramatic increase in cyber incidents caused by both state and non-state actors. The Group recommends a set of voluntary, non-binding norms for responsible state behaviour. Among others, these norms imply that states refrain from internationally harmful cyber activities. In addition, states should not knowingly allow their territory to be used for various internationally malicious cyber operations.

The GGE recommends a set of CCBM that involve points of contact, mechanisms to enhance interstate confidence-building, and measures aimed at transparency and information-sharing regarding trans-national threats, vulnerabilities and best practices. States should seek international co-operation to address vulnerabilities that endanger cross-border critical infrastructures. Co-operation is also recommended to address cyber security incidents and to mitigate cross-border malicious cyber activity. Furthermore, the GGE recommends international co-operation and assistance in cyber security and capacity-building.

With regard to the application of international law to state use of ICT, the GGE identified as international law principles: sovereign equality; the settlement of international disputes by peaceful means; refrain from the threat or use of force in international relations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other states. The GGE urges states not to use proxies for international malicious cyber operations. In addition, states should ensure that their territory is not used by non-State actors to commit such activities. Finally, the GGE underlines the significance of substantiated attribution of malicious cyber incidents.

In 2013, the OSCE adopted an initial set of cyber CBM that would complement the UN measures. In March 2016, a second set of measures was adopted, primarily based on voluntary commitments, information exchange, co-operation and transparency. The OSCE advocates interstate information exchange on the regional and/or sub-regional level to further investigate co-operative measures, processes and mechanisms. Participation of the private sector, academia, centres of excellence and civil society in such activities is encouraged. Furthermore, the formation of public-private partnerships to respond to common security challenges is advocated. The OSCE pays special attention to securing critical infrastructures. Finally, responsible reporting of vulnerabilities to businesses and industry, and their potentially available remedies, is mentioned.

In addition to the UN and OSCE initiatives, various major regional initiatives for cyber CBM have been launched; with varying results. In 2001, the Shanghai Cooperation Organisation (SCO) sent a draft proposal for a code of conduct (CoC) to the UN aiming at an agreement on voluntary, non-binding international cyber norms and rules for state behaviour. Many Western governments opposed the CoC for a variety of reasons. The association of Southeast Asian nations (ASEAN) re-

gional forum (ARF) is one of the main forums for the discussion of cyber CBM in Asia. Their 2015 work plan contains proposals for various activities that show similarities with the OSCE measures. The organisation of American states (OAS) followed a different approach to combat threats to cyber security. Their cyber security strategy contains various (confidence-building) measures with the main objective to respond rapidly to cyber incidents. The OAS strategy focuses on concrete coordination and cooperation measures, protocols and procedures for the exchange of information.

Alongside the UN, OSCE, SCO, ARF and OAS initiatives, the three major cyber power blocks US, Russia and China have also made bilateral agreements, either in the form of a formal treaty or a more informal politically binding arrangement. Rather than addressing worldwide cyber security, these bilateral agreements focus on the mutual disputes between the power blocks.

4. Ten stumbling blocks that hamper multinational agreement on CCBM.

In the absence of legal prohibitions a state seemingly enjoys virtual freedom of action in cyberspace. The large degree of anonymity that cyberspace offers, facilitates anonymous operations, cyber espionage, the use of proxies, knowingly allowing malicious activities, and the conduct of covert operations. These cyber operations, together with the attribution challenge, contribute to interstate distrust, misperception and misunderstanding. In addition, offensive military cyber skills, knowledge and means cannot be distinguished from their defensive equivalents and may also affect non-military, hence civil objects. Aforementioned cyber capabilities are complicating factors that eventually may threaten international peace and stability.

With the UN's ultimate goal to strengthen international peace and security and the ambition to prevent all wars in mind,[328] one would assume that governments swiftly agree on one single set of cyber CBM. To date, however, the wish for international stability and security, and the prevention of war, has not yet led to a set of worldwide acceptable, politically binding set of measures. International agreements are beginning to materialise. However, hitherto, pursuing a set of worldwide acceptable CCBM appears to be a nearly impossible endeavour, with seemingly poor results thus far.

As reaching an agreement on measures is difficult for various reasons, this chapter lists and analyses the various aspects that complicate reaching a global multinational agreement. The stumbling blocks as set out below are based on desk research and observations. To confirm, deny and/or examine these identified potential obstacles, discussions and interviews with individuals and focus groups of appropriate experts were held during national and international conferences, symposia and meetings on this subject. To validate the research and associated conclusions, this paper has been peer reviewed by national and international experts.

4.1. No common cyber terminology. When considering the various CCBM initiatives, one of the most striking features to emerge from the analysis is that agreement on a common cyber terminology already proves to be difficult. Within international organisations such as the UN, NATO, EU, and OSCE, or even within single states, different wording is used to indicate similar terms, whereas similar wording is used to refer to different terms (e.g., cyber security, cybersecurity, information security, ICT security, cyberspace, information space, information warfare, cyber warfare, cyber attack, cyber incident). In addition, states sometimes just interpret similar words differently (e.g., sovereignty, privacy, internal affairs, offensive cyber). The lack of common definitions and different interpretations facilitate misperception; moreover they hamper a sound debate on CCBM. As it is unlikely that global agreement on definitions will be achieved, a focus on transparency of the different interpretations may help reduce misunderstandings.

4.2. A (too) large number of stakeholders. CBM are usually designed and developed according to a predetermined roadmap of which the start-up phase requires a conflict assessment. The assessment should include an overview of the main stakeholders and their individual and common interests, their shared values, and their mutual benefit from co-operation. One of the pitfalls that complicate the cyber CBM development process is the large number of stakeholders.

Previous CBM (e.g., measures concerning nuclear, biological and chemical weapons, or measures involving the limit of conventional or strategic arms) involved only a handful of major powers actually owning those weapons. However, as all states are now connected to cyberspace and cyber attacks may thus originate from everywhere and effects could be achieved worldwide, the amount of

[328] UN document A/S-15/3, Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament, 28 May 1988, p 30

participants that are or should be sitting down at the negotiating table, has increased exponentially. The skills, knowledge or technical level of highly digitalised states vary significantly from less cyber-developed states. The cyber negotiating playing field is, therefore, not level.

CCBM encompass many aspects, such as international law, state sovereignty, territorial integrity, technical features, national security, universal human rights, free flow of information, as well as social, economic, historical and cultural elements. This complexity prevents governments from taking quick and routine decisions. Consequently, CCBM have become subject to international political negotiations, of which the result is a trade-off, and where all relevant players negotiate on every facet.

An additional problem is that cyberspace (i.e. the hardware, software, protocols and data) is not state-owned, but largely privately owned and managed. Moreover, 'the internet' does not even exist. Cyberspace has become a constantly evolving global network of networks that is, to a large extent, in the hands of a variety of private national and international stakeholders with interests in one or more countries. New centres of power, weak hierarchies, overlapping private and public interests, non-state actors with unclear roles, responsibilities and threats, and new types of conflict are influencing traditional international relations. Cyberspace as a new domain of interaction has lead to many changes, such as the involvement of the private sector, new threats to national security, asymmetry, power shifts and disagreement on the influence and control over the management of cyberspace. These developments, particularly triggered by cyberspace, have fundamentally changed the way modern international relations are being established and maintained. Cyberspace has thus grown into a multi-stakeholder realm beyond the traditional Westphalian principle of state sovereignty.[329]

Although the state remains a dominant player in international relations, the CCBM development complexity is compounded by the large number of stakeholders; each with their own concerns, interests, norms and values. This leads towards an apparent paradox: to achieve an optimum result, wide-ranging interaction between (too) large numbers of stakeholders is required. However, these (too) large numbers of stakeholders at the same time hamper this very process. Developing and implementing CCBM thereby becomes a seemingly impossible task.[330]

4.3. Deep mutual distrust. The (too) large numbers of stakeholders is exactly where the danger for the cyber CBM development process lies. CBM intend to create mutual benefits, but may – due to a deep mistrust among the different stakeholders – be perceived as a zero-sum game in which an advantage to other parties is seen as loss of one's own gain. Particularly the level of distrust between the major world powers that are in geopolitical and/or economic competition for influence, may work against effective solutions to create worldwide CCBM. Different values and social, economic, cultural, (national) security or other interests, or just the usual deep mutual distrust appear to be too influential to hinder the swift creation of globally acceptable, politically-binding CCBM.

As long as states' views on duties and responsibilities, anonymous operations, cyber espionage, warfare or weapons, the use of proxies, covert operations, (knowingly allowing) malicious activities, internet governance, privacy and other human rights are too dissimilar, the desired global stability and security in cyberspace will fail to happen. The large degree of anonymity and the attribution problem only further contribute to interstate distrust, misperception and misunderstanding. The use of proxies to evade legal or political responsibility is yet another major barrier.

[329] The formulation of sovereignty was one of the most important intellectual developments leading to the Westphalian revolution. Accessed September 2016: http://www.wwnorton.com/college/polisci/essentials-of-international-relations5/ch/02/summary.aspx

[330] The internet governance discussions involving the transfer of Internet Corporation for Assigned Names and Numbers (ICANN) responsibilities and the discussions about the internet domain name policy revealed a foretaste of multi-stakeholder and multi-interest CCBM discussions to come.

Already in 1998 the Russian Federation (unsuccessfully) proposed an arms-control treaty to the UN that would have banned the use of cyberspace for military purposes.[331] A simple norm to facilitate responsible state behaviour, is it not? Whether the Russian Federation was really striving towards world peace, whether they just experienced a major cyber-technological gap with the USA, or just preferred the stealthy use of proxies, is still unclear. Until 2005, Russia was the only state in favour of the draft resolution, but that same year the tide turned, ironically, because the US started to actually vote *against* the Russian proposal. The US vote appeared to be a game-changer in the process, as the strong contrast between the two states mobilised both the states in favour of, and the states opposing the resolution. In 2009, the count stood at 30 states in favour of the Russian proposal, for the first time including China.[332] One year on, in a likely spirit of pragmatism, the US suddenly changed its policy again and joined the group of supporters. According to Ziolkowski, this switch was made as it allowed the US, from that moment on, to influence the content and wording.[333] Maurer doubts whether the change of position constituted an actual strategic reversal. The move might as well have been made because of the then administration change, and should thus be seen in the light of a general 'policy reset' towards Russia.[334]

In 2001, the Russian Federation and China, supported by Tajikistan and Uzbekistan, launched a combined proposal for a UN-resolution to establish international norms, the earlier mentioned SCO code of conduct. Mainly due to the robust Western opposition this attempt was again unsuccessful. In the view of Western democratic states, a 'simple' norm for responsible behaviour would be that states take responsibility for cyber actions of non-state actors operating from their territory. The combined Russian-Chinese proposal, however, did not contain any text regarding state responsibility for proxies.[335] Finding the greatest common denominator and developing aforementioned 'simple' norms proves to be a challenge.

With regard to the EU's convention on cyber-crime,[336] various influential states, i.e. Russia, Brazil, China and India, have refused to adopt the convention, partially because they did not participate in its drafting, partially because it would fail to protect the rights of individuals and states, and partially because it would not ensure a cyber-crime free cyberspace.[337] In addition, Russia and a number of liked-minded nations (such as the members of the commonwealth of independent states (CIS) and the Shanghai cooperation organisation oppose the convention, arguing that adoption would violate their states' sovereignty.[338] In pursuit of CCBM, the extent to which states might concede a degree of sovereignty in exchange for greater security appears to be a major stumbling block. Rather than finding common values CCBM should, therefore, focus on diminishing the existing distrust. This is yet another seemingly impossible task.

4.4. The use of proxies. Another challenge is related to the use of proxies. Especially in cases where states want to evade or deny their legal or political responsibility, or in cases where offensive cyber activities or other, illegitimate cyber actions would not match with the state's ethical or cultural

[331] Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications*, p 536.
[332] Idem, p 571.
[333] Ibidem.
[334] Tim Maurer, Cyber *Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security*, Discussion Paper 2011-11, Cambridge, Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011, p – 6.
[335] Ibidem.
[336] Council of Europe, *Convention on Cybercrime*, Budapest, November 23, 2001.
[337] Sinha Shalini, *Budapest Convention on Cybercrime – An Overview*, Center for Communication and Governance New Delhi, Legally India, Article 03 March 2016. Accessed September 2, 2016, http://www.legallyindia.com/blogs/budapest-convention-on-cybercrime-an-overview.
[338] Keir Giles, *Russia's Public Stance on Cyberspace Issues*, in *4th International Conference on Cyber Conflict 2012*, edited by Cristian Czosseck, Rain Ottis, Katharina Ziolkowski, NATO CCD COE Publications, Tallinn, 2012, p 65.

norms, a state may hide behind non-state, yet state-sponsored proxy actors. Some hacktivist groups and organised cyber crime elements possess such cyber capabilities that they may even become a threat to the state in which they are located. Czosseck argues that once such a state realises that those elements cannot be effectively combated, that state may as well use their capabilities to carry out cyber activities for them.[339]

A state's lack of knowledge and technology could be compensated by seeking assistance of sophisticated non-state actors with the appropriate cyber capabilities, such as cyber criminals providing 'cyber-crime-as-a-service'. In 2014, Europol's EU Cybercrime Centre (EC3) observed a global trend towards a professional service-based criminal industry, extending the attack capacity to those otherwise lacking the skills or capabilities.[340] These services do not originate from the usual rogue states. Moreover, according to a 2016 SecurityIntelligence (an IBM cyber security company) analysis, the majority of the malicious cyber-crime domains were registered in the US (some fifty percent), whilst the other half are located in the UK, Portugal, Iceland, Russia and the Netherlands.[341]

Malicious governments could motivate criminal actors to change their profit-driven behaviour to more politically-driven action.[342] In addition, especially hacktivists may share common goals with their host state and carry out (malicious) patriotic cyber activities that are condoned or knowingly allowed by their host. Whereas states could thus officially declare to refrain from malicious or offensive cyber warfare activities and the use of cyber-weapons on the international scene, (state-sponsored) proxies could achieve the required effects in their stead.

The main reason for using proxies is the possibility to deny or evade actual state involvement. The large degree of anonymity in cyberspace and the attribution challenge facilitate this practice. Even when a state commits to comply with various norms of state behaviour and CCBM, it could merely make use of proxies to carry out activities in its place.

4.5. Opaqueness. CCBM could aim at reducing distrust and fear by making states' behaviour more predictable. This would mainly involve the exchange of cyber-related information, i.e. military cyber strategies, doctrines, unit sizes, budget, exercises, equipment and arms. In addition, the exchange of information could also require the disclosure – or termination – of yet stealthy and anonymous operations that states are likely keen to preserve. There is a danger that such measures are seen as misleading or just an attempt to manipulate the international CCBM discussion. The possibility to verify information is, therefore, of paramount importance. This would require transparency; yet another major obstacle.

Due to its characteristics and elusive construction, cyberspace is a far cry from being transparent. It is hard to distinguish offensive military cyber capabilities from defensive skills, knowledge and means. In addition, designing, developing, producing and testing of cyber-weapons can be done in a stealthy, non-verifiable manner. Cyber-weapons are thus easy to deny and easy to hide. As a result, guarantees are easy to circumvent and agreements are hard to monitor or verify. The possibility to continuously verify compliance with the agreed provisions is, therefore, lacking. In addition, even if a state would want to support a – yet to develop – verification type mechanism (e.g., by showing its capabilities), such capabilities may then become instantaneously redundant.[343]

[339] Czosseck, *State Actors and their Proxies in Cyberspace*, p 17.
[340] Europol EU Cybercrime Centre, *The Internet Organised Crime Threat Assessment (IOCTA)*, September 29, 2014. Key findings, p – 11. Accessed October 21. 2016. https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
[341] Rick. M. Robinson, *Cybercrime-as-a-Service Poses a Growing Challenge*, September 4, 2016. Accessed October 21, 2016. https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/.
[342] Maurer, *Cyber Proxies and the crisis in Ukraine*, p 86. 21
[343] E.g., revealing zero-days, exploits, vulnerabilities, techniques, would make these useless as a part of, or tool for a cyber-weapon.

Usually under the pretext of national security, national mass surveillance programs also gratefully make use of cyberspace's opaqueness to monitor certain groups of people (i.e. criminals, activists or terrorists), the own population, adversaries, or simply any other sufficiently important person, organisation or state. In 2013, Edward Snowden revealed the existence of the US NSA's PRISM program,[344] a clandestine surveillance program that allows the US government to collect user data from companies like Microsoft, Google, Apple, Yahoo, and others.[345] The NSA uses PRISM to spy on embassies and missions all over the world.[346] These practices are not limited to the US. Worldwide, governments apply these practices to collect and investigate information, but their legality varies and depends on each individual state's national law and judicial system. Whereas espionage is focused and targeted, mass surveillance programs indistinctively harvest data of entire populations, both nationally and internationally. Such surveillance programs thus go well beyond traditional 'tolerated espionage'. It may be obvious that states will not disclose the technical features of their surveillance programs, nor will they reveal who is targeted and what information is collected.

Another area where transparency could play a role is safeguarding cyberspace, in particular the protection of cross-border, internationally interconnected and interdependent critical infrastructures that are crucial to the well-functioning of the international society. The UN GGE 2015 report recommends a set of norms in this direction.[347] Among others, these UN norms for responsible state behaviour imply that states will not conduct or knowingly support cyber activities that intentionally damage critical infrastructures. With regard to the exchange of information, states could join a global early warning system for cyber incidents and provide that system with information about threats, attacks, vulnerabilities and effective remedies. States could agree on mutual assistance with regard to a joint defence, the detection of incidents and the mitigation of attacks. The proposed norms also imply that states should guarantee the integrity of the 'IT-chain', i.e. the hardware, software and protocols. States would thus (guarantee to) not tamper with these elements. Furthermore, states should refrain from the proliferation of malicious cyber tools and techniques.

These intentions are not sufficient in their own right, but essential parts of a wider framework of stability; praiseworthy, however naive. The main challenge with these norms is their voluntary and non-binding character. To effectively fight trans-national cyber crime and cyber terrorism, an international legal framework is required that regulates international cooperation and cross-border law enforcement. This would imply the creation of a worldwide, non-voluntary and legally-binding framework; a seemingly impossible task.

Even more importantly is the fact that CCBM may avert escalation and reduce the chances to an armed conflict, mainly in cases where cyberspace would be destabilised unintentionally. However, the usefulness of these measures is limited in cases where escalation and (armed) conflict is intended. The question is, whether states would be willing to give up their relatively large degree of anonymity in cyberspace and start exchanging information about their behaviour that forms the current threat to international peace and stability. Would states really be willing to give up their anonymous operations, their cyber espionage activities, their use of proxies, their conduct of covert operations and their knowingly allowing the malicious activities of others? Would states really be willing to exchange information about, or simply give up, their offensive military cyber skills, knowledge, means and purposes? Would states really be willing to cease tampering with elements in the 'IT-chain'?

[344] PRISM - Planning tool for Resource Integration, Synchronization and Management.
[345] T.C. Sottek and Joshua Kopstein, *Everything you need to know about PRISM, a cheat sheet for the NSA's unprecedented surveillance programs*, in *The Verge*, July 17, 2013. Accessed October 21, 2016. http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.
[346] Bruce Schneier, *Espionage vs. Surveillance*, in *Schneier on Security*, May 14, 2014. Accessed October 21, 2016. https://www.schneier.com/blog/archives/2014/05/espionage_vs_su.html
[347] UN document A/70/174.

The exchange of the abovementioned cyber-related information would require a high level of transparency, aimed at fostering a better mutual understanding of national capabilities and activities, which may only be achieved when all stakeholders set aside their current distrust and harmonise their yet varying views, interest and values. Would states accept the related monitoring and verification mechanisms and the according hard guarantees (i.e. a legally-binding UN Security Council Resolution)? That would be, in my view, wishful thinking.

4.6. Deliberate use of cyber-weapons. The means and technology to create cyber-weapons are seemingly rather easily available (i.e. computer hardware, some software and an internet connection).[348] Compared to traditional weapon systems, cyber-weapons are relatively cheap. In addition, creating cyber-weapons can be done in a stealthy manner. A cyber-weapon is nothing more than computer code: easy to hide, easy to transport, and thus easy to deny and difficult to detect. Furthermore, the human skills and knowledge to create cyber-weapons are more valuable than the weapon itself. In the case that a state declares to refrain from creating cyber-weapons, it could still invest in the human capacities and technical capabilities to develop such weapons at a later stage. And even if a state neither possesses nor wants to acquire the necessary skills, knowledge or means, capable and willing proxy entities may fill that gap. CCBM ruling out the design, development, production, or testing of cyber-weapons seem, therefore, unlikely or rather impractical to monitor, inspect or verify.

Cyber confidence-building measures may enhance the mutual situational awareness and common understanding, and thus help de-escalate unintentional cyber incidents and prevent interstate armed conflicts. However, when conflicts are triggered intentionally, CBM are of limited use.

In its 2013 and 2015 GGE reports the UN acknowledged that international law applies to cyberspace,[349] but *how* that law applies is yet unclear.[350] In the absence of cyber-specific legal prohibitions a state thus seemingly enjoys freedom of action regarding military cyber operations or the use of cyber-weapons. Several states already have, or are developing computer code with a potentially deadly and devastating effect similar to traditional weapons. Adversarial states might not be able to reach their opponents with traditional weapons. However, due to the virtually unlimited reach of cyber-weapons, they now can. A pledge to refrain from the use of relatively cheap and effective cyber means would, therefore, not be attractive for these states.

4.7. 'No first use' declaration unfeasible. States might consider complying with a 'no first use policy'. Yet another complication involves practical snags with such a 'no first use' declaration. States are namely also involved in law enforcement and intelligence activities in cyberspace. The skills, knowledge, methods and means used in the latter areas are fairly similar to those used for cyberwarfare. Adhering to the principle of 'no first use' would not only mean that a state may not merely (first) use cyber means for warfare purposes. Moreover, it would also imply that a state may not use these cyber means for legitimate law enforcement and (tolerated) espionage purposes.

Furthermore, international humanitarian law influences a state's warfare options. When planning for a legitimate attack, a state must consider, among other things, the proportionality of the weapons to be used.[351] If a state has the choice between using a truly destructive kinetic weapon or a less-

[348] The appropriate skills and knowledge to use these means may still be challenging, but to a large extent also available online, as guideline or even as a service (e.g., cybercrime-as-a-service).
[349] such as the Charter of the UN, Law Of Armed Conflict and International Humanitarian Law.
[350] Elaine Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?* in *Lawfare*, September 12, 2015. Accessed October 18, 2016. https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.
[351] International Committee of the Red Cross, *Customary International Humanitarian Law (IHL) Database, 2016, Chapter 4: Proportionality in attack, Rule 14*: Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians,

destructive, less-lethal cyber-weapon that could achieve similar effects, the use of such a cyber-weapon must be considered. Therefore, norms or CCBM that would exclude particular cyber skills, techniques or means, or which would entail a 'no first use' declaration, seem unrealistic.

4.8. Excluding (cyber) targets from (cyber) attacks unfeasible. Another difficulty concerns excluding particular (cyber) targets from (cyber) attacks. The international community has concluded that existing international law, and in particular the Charter of the UN, is applicable to cyberspace.[352] The existing Law of Armed Conflict (LOAC) already specifies restraints and constraints with regard to what may, and may not be targeted. With regard to traditional weapons, the LOAC protects, and rightly so, civilian objects and persons. However, even then, this law does not completely rule out, for example, civilian critical infrastructures from traditional attacks.[353] It seems unrealistic to exclude particular cyber *targets* by the means of confidence-building measures, if not particularly excluded in an internationally accepted and implemented law. In a similar vein, it is illogical to exclude particular targets from a cyber *attack*. This would mean that a target may not be attacked by cyber-weapons, whereas the use of any other (kinetic) weapon would be allowed. Non-binding CBM that, beyond the current existing international law, exclude certain (cyber) targets from (cyber) attacks seem, therefore, hardly feasible.

4.9. Cyberspace's features. The previous paragraphs showed various aspects that help explain why reaching a multinational agreement on CCBM is difficult. In addition, cyberspaces features may also give rise to complications concerning the earlier mentioned OSCE's eleven characteristics of successful CBM. The influence of cyberspace on three of these characteristics will complicate the development and implementation of cyber CBM, namely local ownership, multi-level implementation and verification.

The successful long-term implementation of CBM depends on the voluntary engagement and real commitment of all parties. To that extent the interests, concerns, needs and priorities of all relevant parties must be taken into account. The given (too) large numbers of stakeholders and the wide variety of their interests will pose a barrier to a voluntary engagement and real commitment. CCBM can be developed top-down or bottom-up, but involvement of both government structures and civil society at large is an essential prerequisite for lasting success. Again, the (too) large numbers of public and private stakeholders, with their deep mutual mistrust and diverging values and interests, will hamper the CCBM development process. In addition, particularly in cases where reciprocity is expected, verification would be an important aspect in reducing parties' fear and mistrust. Due to cyberspace's elusive character, its large degree of anonymity and opaqueness, precisely the verification of previous commitments is problematic.

4.10. No urgency to quickly reach an agreement. Although various CCBM developing initiatives have been launched, states appear to be satisfied with the current international situation. Macintosh explains that, when the conditions are right (i.e. supportive), the process of developing valid CBM may give a boost to promoting changes in security thinking.[354] However, the challenge with developing cyber confidence-building measures is that these conditions still appear to be far from supportive.

---

damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited. From: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter4_rule14

[352] UN Document A/68/98, p 2.

[353] International Committee of the Red Cross, *Customary International Humanitarian Law (IHL) Database*, 2016, *Chapter 2: Distinction between Civilian Objects and Military Objectives, Rule 10:* Civilian objects are protected against attack, unless and for such time as they are military objectives. Accessed August 2016, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter2

[354] James Macintosh, *Confidence Building in the Arms Control Process: A Transformation View*, Ottawa, Canada: Department of Foreign Affairs and International Trade, Arms Control and Disarmament Studies Number 2, 1996. JX 1974.M32 1996.

Only when at least some states share a great dissatisfaction with the current international cyber security situation, confidence building may help changing their mutual security relationships.[355] Although many states have recognised the potential cyber security risks to their now interconnected economies, and although states have acknowledged the need for cooperation, devastating major cyber-attacks resulting in many casualties or severe damage, have not yet taken place. Despite various warnings we have not yet suffered from a cyber Armageddon,[356] a cyber Pearl Harbour,[357] a cyber doomsday,[358] or a cyber 9/11.[359] Governments and other, non-state actors would be willing to quickly develop and implement CCBM if only the urgency would be really obvious. To date, this urgency to quickly reach an agreement seems lacking. Unless one or more cyber-catastrophes soon occur, developing a set of worldwide acceptable politically-binding CCBM remains a lengthy, if not impossible trajectory.

[355] Ibidem.
[356] James Clapper, *US Spy Chief Warns of Space Wars, North Korean Nukes, and Cyber Threats*, Vice News, February 9, 2016. Accessed 4 May 2016, https://news.vice.com/article/us-spy-chief-warns-of-space-wars-north-korean-nukes-and-cyber-armageddon.
[357] Hamre, John. *The 'electronic Pearl Harbor'*, Politico Magazine, September 9, 2015, Accessed May 4, 2016, http://www.politico.com/agenda/story/2015/12/pearl-harbor-cyber-security-war-000335.
[358] NBC news article 'Obama's doomsday cyberattack unrealistic – experts say' http://www.nbcnews.com/id/48265682/ns/technology_and_science-security/t/obamas-doomsday-cyberattack-scenario-unrealistic-experts-say/#.VyoRmvmLSM8
[359] Bert Koenders, *Speech at the Münchner Sicherheitskonferenz*, The Hague, February 12, 2016, Accessed July 2016, https://www.rijksoverheid.nl/documenten/toespraken/2016/02/12/toespraak-van-minister-koenders-munchner-sicherheitskonferenz

5. Conclusions and recommendation

5.1. Conclusions. Malicious cyber activities carry the risk of misperception and unintended escalation into a military conflict and thus threaten the international peace and stability. Despite the various initiatives, to date, the wish for international security and the prevention of war, has not yet led to a set of worldwide acceptable, politically-binding cyber confidence-building measures. This research paper identified ten obstacles that hamper the CCBM development and implementation process:

1. The lack of common definitions facilitates misperception and hampers a sound debate on CCBM.

2. (Too) large numbers of stakeholders, each with their own concerns, interests, norms and values, are needed to achieve an optimum result, but also hamper the CCBM trajectory.

3. A deep mutual distrust, and different values, social, economic, cultural, (national) security or other interests appear to hinder the CCBM process.

4. By using proxies, states may evade or deny their legal or political responsibilities for offensive cyber activities or other, illegitimate cyber actions that would normally not match their norms.

5. Transparency may reduce distrust and fear, but states are not likely to give up their large degree of anonymity in cyberspace to start exchanging information about jeopardising activities.

6. CCBM ruling out the design, development, production, or testing of cyber-weapons seem unlikely. In addition, when conflicts are triggered intentionally, CCBM are of limited use.

7. Norms or CCBM that would exclude particular cyber skills, techniques or means, or which would entail a 'no first use' declaration, seem unrealistic.

8. Introducing non-binding CCBM that, beyond the current international Law of armed conflict, will exclude specific (cyber) targets from (cyber) attacks, seem unfeasible.

9. Three of OSCE's characteristics for successful CBM, namely local ownership, multi-level implementation and verification can hardly be complied with, due to cyberspace's features.

10. Devastating major cyber-incidents with a worldwide impact have not yet taken place, resulting in a lower sense of urgency to develop and implement worldwide CCBM.

In theory, all necessary ingredients for a significant contribution of CCBM to mitigate the risk of cyber incidents into interstate armed conflict are within the power of states. States: (1) have the legal mandate to launch military operations in cyberspace; (2) should have the monopoly on the legitimate use of violence (power) in cyberspace, while at the same time proxy-actors also play a significant role; (3) have the authority to act against non-state proxy actors operating from their territory; (4) establish international relations; (5) and negotiate on CCBM.

In practice, the level of distrust and fundamental different values between the world powers appear to be so high that a greatest common denominator can hardly be found, and easy agreement on even 'simple' norms cannot be reached. Conflicting political, geopolitical, social, economic, religious or cultural agenda's, covert military actions, espionage, mass surveillance and competition for global influence hamper the discussion of cyber-security and CCBM.

The final conclusion is that, unless game-changing worldwide cyber-catastrophes occur, it is unlikely that worldwide acceptable, effective, politically-binding CCBM will be created and, moreover, implemented.

5.2. Recommendation for further research. As regards fields of interest for further research, the following may be considered.

- The extent to which the ten identified stumbling blocks could be eliminated;
- The feasibility of bottom-up, top-down or various regional politically-binding CCBM;
- The feasibility of the development and implementation of legally-binding cyber CBM;
- The feasibility of an international attribution agency;
- The feasibility of cyber-specific international law.

5.3. Reflection. Will there ever be worldwide measures? Finding global consensus on any given subject has always been a challenge in the past, is a challenge at present, and will likely be a challenge in the future. Achieving worldwide cyber CBM will be no exception to that rule. The existing geopolitical rivalries play a crucial role in any discussion. Cyber-related decisions do not exist outside other geopolitical concerns. The UN acknowledges that a detailed universal model of CBM is impractical. Confidence-building measures should thus be tailored to a specific situation or region. This contradicts UN GGE's simultaneous aspiration of all-encompassing global cyber CBM.

Cyberspace is a fairly new domain and the developments around (cyber) confidence-building measures occurred mainly in the past few years. In discussing whether cyber is any different to other disciplines in this process, recent arguments are being put forth, primarily by diplomats, that progress has been even faster than countries in fact expected. The question is whether this optimism is justified also in the longer run, in the absence of actual progress and success. It is nevertheless essential to continue the diplomatic efforts, the negotiating process and the subsequent discussions. These are all parts of a larger strategic framework that in their own right implicitly constitute (cyber) confidence-building measures.

The discussions around cyber confidence-building measures are only partially a technological challenge. To a much larger extent it is a human behaviour problem, primarily related to trust and confidence in both technology and other people.

Annex A – Abbreviations

APEC	Asia-Pacific Economic Cooperation
APT	Advance Persistent Threat
ARF	Association of Southeast Asian Nations Regional Forum
ASEAN	Association of Southeast Asian Nations
CBM	Confidence-Building Measures
CCBM	Cyber Confidence-Building Measures
CCD COE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CICTE	Inter-American Committee Against Terrorism
CIS	Commonwealth of Independent States
CoC	Code of Conduct
CSBM	Confidence- and Security-Building Measures
CSIRT	Computer Security Incident Response Teams
DNC	Democratic National Committee
DoS	Denial of Service
EC3	EU Cybercrime Centre
EDA	European Defence Agency
EU	European Union
FBI	Federal Bureau of investigation
FIRST	Forum of Incident Response and Security Teams
GGE	Group of Governmental Experts
ICANN	Internet Corperation for Assigned Names and Numbers
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
IHL	International Humanitarian Law
IOCTA	Internet Organised Crime Threat Assessment
ISIL	Islamic State of Iraq and the Levant
IT	Information Technology
IP	Internet Protocol
LOAC	Law Of Armed Conflict
MISP	Malware Information Sharing Platform
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
NRRC	Nuclear Risk Reduction Centre
NSA	National Security Agency
OAS	Organisation of American States
OSCE	Organisation for Security and Co-operation in Europe
OT	Operational Technology
PMP	Permanent Monitoring Panel
PRISM	Planning tool for Resource Integration, Synchronization and Management
SCO	Shanghai Cooperation Organisation
UN	United Nations
UNGA	United Nations General Assembly
UNIDR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
UNSC	United Nations Security Council
US	United States

Annex B – Bibliography

Allison, Graham T. *The American Political Science Review, Conceptual models and the Cuban missile crisis,* Volume 63, Issue 3 (Sep 1969), p. 689-719. DOI: http://dx.doi.org/10.2307/1954423.

Arnold Kraesten, and Dalmijn, Arthur. *Working paper in preparation of The Netherlands Doctrine for Military Cyber Operations,* draft Netherlands Ministry of Defence restricted version August 2016.

ASEAN, Regional Forum *Work Plan on security of and in the use of information and communications technologies (ICTs)*, 7 May 2015, Accessed August 2016, http://aseanregionalforum. asean.org/files/library/Plan%20of%20Action%20and%20 Work%20Plans/ARF%20Work%20Plan%20on%20 Security%20of%20and%20in%20the%20Use%20of%20Information %20and%20Communications%20Technologies.pdf.

ASEAN, Regional Forum on Operationalising Confidence Building Measures for cooperation during cyber-incident response, *Concept-paper,* Kuala Lumpur 2-3 March 2016.

Argent Pierre d', and N. Susani. *United Nations, Purposes and Principles,* in *The Max Planck Encyclopedia of Public International Law*, edited by Rüdiger Wolfrum, Oxford University Press, online edition, (n 105) 11.

Aust, Anthony. *Handbook of International Law*, London School of Economics and Kendall Freeman Solicitors, Cambridge: Cambridge University Press, 2005.

Benschop, Albert. *Cyberoorlog, slagveld internet*, Tilburg, Uitgeverij de Wereld, 2013.

Besson, Samantha. *Sovereignty* in MPEPIL (n 2) MN 2; cf Epping and Gloria (n 143) § 26 MN 13.

Boulet, Gertjan. *Cyber Operations by Private Actors in the Ukraine-Russia Conflict: From Cyber War to Cyber Security*, in *American Society of International Law*, Volume 19, Issue 1, January 7, 2015. Accessed October 16, 2016. https://www.asil.org/insights/volume/19/issue/1/cyber-operations-private-actors-ukraine-russia-conflict-cyber-war-cyber.

Broeders, Dennis. *The public core of the Internet,* An international agenda for Internet governance, Amsterdam: Amsterdam University Press, 2015.

Brunner, Jordan. *Iran Has Built an Army of Cyber Proxies*, in *The Tower Magazine*, Issue 29, August 2015. Accessed October 14, 2016, http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/.

Buchan, Russell. *The International Legal Regulation of State-Sponsored Cyber Espionage,* in *International Cyber Norms, Legal, Policy & Industry Perspectives*, edited by Anna-Maria Osula and Henry Rõigas, NATO CCD COE Publications, Tallinn 2016.

Choucri, Nazli. *Cyberpolitics in International Relations*, Massachusetts Institute of Technology 2012, the MIT Press, Cambridge, Massachusetts London, England, 2012.

Clausewitz, Carl von. *Vom Kriege: hinterlassenes Werk*, Frankfurt/M, Berlin, Wien: Ullstein 1832, (1980).

Clapper, James. *US Spy Chief Warns of Space Wars, North Korean Nukes, and Cyber Threats*, Vice News, February 9, 2016. Accessed 4 May 2016, https://news.vice.com/article/us-spy-chief-warns-of-space-wars-north-korean-nukes-and-cyber-armageddon.

Council of Europe, *Convention on Cybercrime*, Budapest, November 23, 2001.

Czosseck, Christian. *State Actors and their Proxies in Cyberspace,* in P*eacetime Regime for State Activities in Cyberspace,* edited by Katharina Ziolkowski, International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn, 2013.

Deibert, Ronald J. *The geopolitics of internet control: Censorship, sovereignty, and cyberspace,* in *The Routledge handbook of internet politics* (2009), edited by Andrew Chadwick and Philip N. Howard.

Elkind, Peter, *Inside the hack*, Fortune Special Investigation Report, Fortune Magazine (online version), Accessed August 2016 http://fortune.com/sony-hack-part-1/

EU Commission, *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Rev 2, 2013/0027 (COD), Brussels, 18 December 2015.

Europol EU Cybercrime Centre, *The Internet Organised Crime Threat Assessment (IOCTA)*, September 29, 2014. Accessed October 21, 2016. https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

Farivar, Cyrus. *A Brief Examination of Media Coverage of Cyberattacks* (2007 - Present), in *The Virtual Battlefield: Perspectives on Cyber Warfare'*, edited by Cristian Czosseck & Kenneth Geers, Amsterdam: IOS Press. doi:10.3233/978-1-60750-060-5-182.

Farnsworth, Timothy. *China and Russia Submit Cyber Proposal*, Arms Control Association, November 2, 2011. Accessed May 2016, https://www.armscontrol.org/act/2011_11/China_and _Russia_Submit_Cyber_Proposal.

Fox News article, *Cyber Spy Networks Hacks Computers in 103* Countries, March 30, 2009. Accessed October 14, 2016, http://www.foxnews.com/story/2009/03/30/cyber-spy-network-hacks-computers-in-103-countries.html

Gayken, Sandro. *Blaming Russia For the DNC Hack Is Almost Too Easy*, August 1, 2016, Accessed August 2016, http://blogs.cfr.org/cyber/2016/08/01/blaming-russia-for-the-dnc-hack-is-almost-too-easy/.

Geers, Kenneth. *Cyber War in Perspective: Russian Aggression against Ukraine'*, NATO CCD COE Publications, Tallinn, 2015.

Geiß, Robin and Lahmann, Henning. *Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention*, in *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* edited by Katharina Ziolkowski, NATO CCD COE Publication, Tallinn, 2013.

Genugten, Willem J.M. van. *Handhaving van wereldrecht: Een kritische inspectie van valkuilen en dilemma's*. Nederlands Juristenblad, (2010) 85(1), 44-46.

Giles, Keir. *Russia's Public Stance on Cyberspace Issues*, in *4th International Conference on Cyber Conflict 2012*, edited by Cristian Czosseck, Rain Ottis, Katharina Ziolkowski, NATO CCD COE Publications, Tallinn, 2012.

Greenberg, Andy, *FBI Director: Sony's 'Sloppy' North Korean Hackers Revealed Their IP Addresses*, in *Wired Magazine*, July 1, 2015, Accessed October 15, 2016, https://www.wired.com/2015/01/fbi-director-says-north-korean-hackers-sometimes-failed-use-proxies-sony-hack/.

Greenwood, Christopher. *Oxford International Public Law*, Article on Self-Defence, Anticipatory Self-Defence, last updated April 2011, Max Planck Encyclopedia of Public International Law [MPEPIL], http://opil.ouplaw.com/view/10.1093/law:epil/ 9780199 231690/law-9780199231690-e401.

Hamre, John. *The 'electronic Pearl Harbor'*, Politico Magazine, September 9, 2015, Accessed May 4, 2016, http://www.politico.com/agenda/story/2015/12/pearl-harbor-cyber-security-war-000335.

Heintschel von Heinegg, Wolff. *Legal Implications of Territorial Sovereignty in Cyberspace*, in *Proceedings of the 4th International Conference on Cyber Conflict*, edited by Christian Czosseck Rain Ottis and Katharina Ziolkowski, NATO CCD COE Publication (2012).

Iasiello, Emilio. *Are Cyber Weapons Effective Military Tools*?, in *Military and Strategic Affairs*, Volume 7, No. 1, March 2015. Accessed October 16, 2016, http://www.inss.org.il/uploadImages/systemFiles/2_Iasiello.pdf

International Committee of the Red Cross, *Customary International Humanitarian Law (IHL) Database*, 2016. Accessed August 2016, https://ihl-databases.icrc.org/customary-ihl/eng/docs/home.

Inter-American Committee Against Terrorism (CICTE), *Declaration Protection of Critical Infrastructure From Emerging Threats*, March 23, 2015, Accessed October 18, 2016, https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

Inter-American Committee Against Terrorism (CICTE), *Declaration: Strengthening Cyber-Security in the Americas*, March 9, 2012. Accessed October 18, 2016, *http://www.state.gov/p/wha/rls/221498.htm*

Jellenc, Eli. *Explaining the Global Cyber Arms Race: Strategic Rivalry and Securitization of Cyberspace among Nation*-States, in *The Proceedings of the 11th European Conference on Information Warfare*, Laval, France, July 6-7, 2012. Accessed August 2012 from: http://www.academia.edu/7664607/Explaining_the_Global_Cyber_Arms_Race_Strategic_Rivalry_and_Securitization_of_ Cyberspace_among_Nation-States.

Kallberg, Jan and Thuraisingham, Bhavani. *From Cyber Terrorism to State Actors' Covert Cyber Operations*, ResearchGate, March 2013, Accessed August 2016, DOI: 10.1016/B978-0-12-407191-9.00019-3.

Koenders, Bert. *Opening speech*, Global Conference on Cyber Security, The Hague, April 16, 2015. Accessed May 4, 2016, https://www.government.nl/documents/speeches/ 2015/04/16/opening-speech-gccs-bert-koenders

Koenders, Bert. *Speech at the Münchner Sicherheitskonferenz*, The Hague, February 12, 2016, Accessed July 2016, https://www.rijksoverheid.nl/documenten/toespraken/2016/02/12/toespraak-van-minister-koenders-munchner-sicherheitskonferenz.

Korzak, Elaine. *The 2015 GGE Report: What Next for Norms in Cyberspace?* in *Lawfare*, September 12, 2015. Accessed October 18, 2016. https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.

Lewis, James Andrew. *Confidence-building and international agreement in cybersecurity*, in *Confronting Cyberconflict*, UNIDIR Disarmament Forum 4, 2011, Accessed May 4, 2016, https://citizenlab.org/cybernorms2012/Lewis2011.pdf.

Lewis, James Andrew. The Cyber War Has Not Begun, Center for Strategic and International Studies (CSIS), March 2010. Accessed July 2016, http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf.

Macintosh, James. *Confidence Building in the Arms Control Process: A Transformation View*, Ottawa, Canada: Department of Foreign Affairs and International Trade, Arms Control and Disarmament Studies Number 2, 1996. JX 1974.M32 1996.

Mason, Simon and Siegfried, Matthias. *Confidence Building Measures (CBMs) in Peace Processes* in *Managing Peace Processes: Process related questions. A handbook for AU practitioners*, Volume 1, African Union and the Centre for Humanitarian Dialogue, 2013: 57-77.

Tim Maurer, Cyber *Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security*, Discussion Paper 2011-11, Cambridge, Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

Maurer, Tim. *Cyber Proxies and the crisis in Ukraine*, in *Cyber War in Perspective: Russian Aggression against Ukraine'*, edited by Kenneth Geers, NATO CCD COE Publications, Tallinn, 2015.

Maybaum, Markus. *Technical Methods, Techniques, Tools and Effects of Cyber Operations*, in *Peacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, *International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn, 2013.

McKay, Angela, Jan Neutze, Paul Nicholas, Kevin Sullivan. *International Cybersecurity Norms Reducing conflict in an Internet-dependent world*. http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_ Cybersecurity_%20Norms.pdf

Ministry of Security and Justice, National Cyber Security Centre, *Cyber Security Assessment Netherlands (CSAN) 4 - 2014*, The Hague, The Netherlands, October 2014.

Ministry of Security and Justice, National Cyber Security Centre, *Cyber Security Assessment Netherlands (CSAN) 2015*, The Hague, The Netherlands, November 2015.

Minnick, Wendell. *Chinese businessman pleads guilty of spying on F-35 and F-22*, in *Defense News*, March 24, 2016, Accessed October 14, 2016, http://www.defensenews.com/story/breaking-news/2016/03/24/chinese-businessman-pleads-guilty-spying-f-35-and-f-22/82199528/.

NATO, *Wales Summit Declaration*, September 2014, Accessed August 2016, http://www.nato.int/cps/en/natohq/official _texts _112964.htm.

Netherlands, *Cyber Defence Strategy*, Ministry of Defence, The Hague, The Netherlands, June 2012.

Netherlands, *National Cyber Security Strategy 2, from awareness to capability*, Ministry of Security and Justice, National Coordinator for Security and Counterterrorism, The Hague, The Netherlands, 28 October 2013.

Norton Cybercrime Report, *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually*, Symantec Press Release, September 7, 2011. Accessed April 28, 2016, https://www.symantec.com/about/newsroom/press-releases/2011/symantec_0907_02.

OAS, *Adoption of a comprehensive inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinair approach to creating a culture of cybersecurity*, AG/RES. 2004 (STATEIV-O/04), 8 juni 2004, Accessed August 2016, http://www.oas.org/STATEIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cy-bersecurity.htm.

OSCE, *Conference on Security Co-operation in Europe: Final Act*, Conference on Security Co-operation, Helsinki, 1975, http://www.osce.org/helsinki-final-act?download=true.

OSCE, *Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1106 (Organization for Security and Co-operation in Europe, Permanent Council, 975th Plenary Meeting, 3 December 2013.

OSCE, *Decision No 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1202, Organization for Security and Co-operation in Europe, Permanent Council, 1092nd Plenary Meeting, 10 March 2016.

OSCE, *Guide on Non-Military Confidence-Building Measures (CBMs)*, Organization for Security and Co-operation in Europe, Vienna, 2012, Accessed August 2016, http://www.osce.org/cpc/91082?download=true.

OSCE, *Document of the Stockholm Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation in Europe*, Organization for Security and Co-operation in Europe, 19 September 1986. Accessed August 2016, http://hrlibrary.umn.edu/peace/docs/stockholm1986.html.

OSCE, *Vienna Document 1990 of the Negotiations on Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Vienna Meeting of the Conference on Security and Co-operation in Europe*, Organization for Security and Co-operation in Europe, Vienna, 17 November 1990. Accessed August 2016, http://www.osce.org/fsc/41245?download=true.

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

Oxman, B.H. Jurisdiction of States, in The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, Oxford University Press, online edition, (n 2) MN 3. Accessed August 2016, http://opil.ouplaw.com/home/EPIL.

Pawlak, Patryk. *Confidence-Building Measures in Cyberspace: Current Debates and Trends*, in *International Cyber Norms, Legal, Policy & Industry Perspectives*, edited by Anna-Maria Osula and Henry Rõigas, NATO CCD COE Publications, Tallinn, 2016.

Pawlak, Patryk. *Cyber Diplomacy: Cyber-Confidence-Building Measures*, European Parliamentary Research Service, Members' Research Service PE 571.302, briefing to the European Parliament, October 2015.

Pirker, Benedikt. *Territorial Sovereignty and Integrity and the Challenges of Cyberspace,* in: *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski, NATO CCD COE Publication, Tallinn 2013.

Randelzhofer, A. and Dörr, O. *Article 2(4)* in *The Charter of the United Nations* 3rd edition, volume 1, edited by B. Simma et al., Oxford University Press, 2012.

Reuters World News, *Chinese economic cyber-espionage plummets in U.S.: Experts*, June 21, 2016. Accessed October 2016, http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D

Richardson, John C. Stuxnet as Cyberwarfare Applying the Law of War to the Virtual Battlefield, Social Science Research Network, 2011.

Rid, Thomas. *Cyber War Will Not Take Place*, Journal of Strategic Studies (2012), 35:1, 5-32. Accessed August 2016, DOI: 10.1080/01402390.2011.608939.

Rid, Thomas and Buchanan, Ben. *Attributing Cyber Attacks*, Journal of Strategic Studies 38 (2014): 4-37. Accessed August 2016, DOI: 10.1080/01402390.2014.977382.

Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez, RAND Europe, *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) prepared for the European Defence Agency*, unclassified summary, March 2013. Accessed August 2016, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR286/RAND_RR286.pdf.

Robinson, Rick. M. *Cybercrime-as-a-Service Poses a Growing Challenge*, September 4, 2016. Accessed October 21, 2016. https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/.

Rõigas, Henry and Tomáš Minárik, *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, in *Incyder News*, August, 2015. Accessed October 18, 2016, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

Sanger, David E. *U.S. Cyberattacks Target ISIS in a New Line of Combat*, The New York Times, April 24, 2016, Accessed October 9, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=1.

Sanger, David E. and Perlroth, Nicole. *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, The New York Times, December 17, 2014, Accessed August 2016 http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0.

Schmitt. Michael N. (ed.). *Tallinn manual on the international law applicable to cyber warfare* prepared by the international group of experts at the invitation of the NATO cooperative Cyber Defence Centre of Excellence: Cambridge University Press, 2013.

Schmitt, Michael N. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework'* (1999) 37 Columbia Journal of Transnational Law (3) 885, 913 and 919; Stein and Marauhn.

Schneier, Bruce. *Espionage vs. Surveillance*, in *Schneier on Security*, May 14, 2014. Accessed October 21, 2016. https://www.schneier.com/blog/archives/2014/05/espionage_vs_su.html

Schneier, Bruce. *Major NSA/Equation Group Leak*, in *Schneier on Security* blog, August 16, 2016. Accessed October 2016. https://www.schneier.com/blog/archives/2016/08/major_nsaequati.html

Shalini, Sinha. *Budapest Convention on Cybercrime – An Overview*, Center for Communication and Governance New Delhi, Legally India, Article 03 March 2016. Accessed September 2, 2016, http://www.legallyindia.com/blogs/budapest-convention-on-cybercrime-an-overview.

Simma, Bruno, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus (editors) and Editor Nikolai Wessendorf (assistant editor), *Oxford Commentaries on International Law, The Charter of the United Nations*, 3rd Edition Volume 1, Oxford University Press, 2012.

Songip, Ahmad Rahman, Z. Md Zaki, K. Jusoff, J. Prebagaran and Ng. Boon-Beng, *Cyberspace: The Warfare Domain*, World Applied Sciences Journal 21 (1): 01-07, 2013. ISSN 1818-4952, IDOSI Publications, 2013, DOI: 10.5829/idosi.wasj.2013.21.1.2825.

Sottek, T.C. and Joshua Kopstein, *Everything you need to know about PRISM, a cheat sheet for the NSA's unprecedented surveillance programs*, in *The Verge*, July 17, 2013. Accessed October 21, 2016. http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

Spiegel Staff, *Documents Reveal Top NSA Hacking Unit*, in *Spiegel Online International*, December 29, 2013. Accessed October 16, 2016. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

Tikk-Ringas, Eneken. *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, Ict4Peace Cyber Policy Process Brief. http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

UN document A/51/182, *Report of the Disarmament Commission, annex F, the Guidelines for appropriate types of confidence-building measures and for the implementation of such measures on a global or regional level*, 1 July 1996. Accessed August 2016 http://www.un.org/Depts/ddar/discomm/2102.htm#tf.

UN document A/65/201, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 30 July 2010.

UN document A/66/176, *Information on confidence-building measures in the field of conventional arms*, 25 July 2011.

UN document A/66/359, *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*, 14 September 2011.

UN document A/68/98, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013.

UN document A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015.

UN document A/S-15/3, *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament*, 28 May 1988.

US Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, Mat 19, 2014. Accessed October 19, 2016, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

US Department of State, *Declaration: Strengthening Cyber-Security in the Americas*, March 9, 2012. Accessed October 18, 2016, http://www.state.gov/p/wha/rls/221498.htm.

US Department of State International Security Advisory Board, *Final Report of the International Security Advisory Board (ISAB) on U.S.-Russia Relations*, December 9, 2014. http://www.state.gov/documents/organization/235118.pdf

Vaishnav, Chintan, Nazli Choucri and David Clark. *Cyber international relations as an integrated system*, in *Environment System & Decisions (2013)* 33: 561–576, Accessed August 20165, DOI 10.1007/s10669-013-9480-3.

Valentino-DeVries, Jennifer and Danny Yadron. *Cataloging the World's Cyberforces*, Wall Street Journal, October 11, 2015. Accessed August 2016, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

Veenendaal, Matthijs, Kadri Kaska, Henry Rõigas and Can Kasapoglu. *DNC Hack: An Escalation That Cannot Be Ignored*, NATO CCD COE News Article, August 5, 2016. Accessed August 2016, https://ccdcoe.org/dnc-hack-escalation-cannot-be-ignored.html.

Warren Harold, Scott, *The US-China Cyber Agreement, a good first step*, RAND corporation, August 1, 2016. Accessed August 2016 http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.

Wei, Yuxi. *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty*, Jackson School of International Studies, University of Washington, June 21, 2016, Accessed August 2016, https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/.

Wegener, Henning. *Information Security Permanent Monitoring Panel World Federation of Scientists*, in *International Seminar on Nuclear War and Planetary Emergencies*, edited by Richard Ragaini, 45th Session: The Role of Science in the Third Millennium, Singapore: World Scientific Publishing Company, 2013.

Wegener Henning, William A. Barletta, Olivia Bosch, Dimitry Chereshkin, Ahmad Kamal, Andrey Krutskikh, Axel H.R. Lehmann, Timothy L. Thomas, Vitali Tsygichko, Jody R. Westby. *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report and Recommendations, World Summit on Information Society, Geneva 2003 – Tunis 2005, Document WSIS-03/GENEVA/CONTR/6-E 19 November 2003.

White House, the, Office of the Press Secretary. *Fact sheet 'President Xi Jinping's State Visit to the United States*, September 25, 2015. Accessed August 2016, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States.

White House, the. Office of the Press Secretary. *Factsheet US-Russian agreement on cooperation on information and communications technology security*, 17 June 2013. Accessed August 2016, https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

Zannier, Lamberto. *Cyber/ICT security: building confidence'*, in Security Community, the OSCE Magazine, Issue 2, 2014.

Zetter, Kim. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, in Wired Magazine, November 7, 2011. Accessed October 8, 2016, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/1.

Zetter, Kim. *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*, in Wired magazine, March 25, 2013. Accessed October 8, 2016, https://www.wired.com/2013/03/stuxnet-act-of-force/

Zetter, Kim. *NSA's Decade-Long Plan to Undermine Encryption Includes Backdoors, Stolen Keys, Manipulating Standards*, in *Wired Magazine*, May 9, 2013. Accessed October 16, 2016. https://www.wired.com/2013/09/nsa-backdoored-and-stole-keys/

Zetter, Kim. *The evidence that North Korea hacked Sony is flimsy*, in Wired Magazine, December 17, 2014. Accessed October 14, 2016, https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/.

Ziolkowski, Katharina. *Confidence Building Measures for Cyberspace – Legal Implications*, in *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski, NATO CCD COE Publication, Tallinn, 2013.

Ziolkowski, Katharina. *General Principles of International Law as Applicable in Cyberspace*, in *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski, NATO CCD COE Publication, Tallinn, 2013.

Ziolkowski, Katharina (editor). Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn, 2013.