**Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures**

*Henning Wegener[[1]](#footnote-1)*

The Permanent Monitoring Panel on Information Security of the World Federation of Scientists has from its inception geared its work to the overriding issues of harnessing cyber conflict, and to the organizational challenge of creating a universal order of cyberspace. We were convinced that the cyber sphere is, if not a lawless space, at least one that lacks a comprehensive legal framework to manage and control the all-pervasive, infinite potential of digital technologies. Consequently, there is little or no ability to effectively control the escalation of cyber conflict, and there is no common understanding of how the existing norms of international law would apply — if at all. A dangerous, precarious state of affairs, which our group has never ceased to analyze and denounce. From the beginning of our activity, we have argued that a comprehensive international legal framework is required to fill this void, establishing norms and rules for adequate, responsible state behavior in order to ensure and guarantee the peaceful use of cyber space. Our first major document, “Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar”[[2]](#footnote-2) reflects that approach. At that time, we ambitiously called for a UN-led effort to create a Comprehensive Law of Cyberspace. Our erstwhile colleague Ambassador Kamal has later fleshed out this project in a book “The Law of Cyber-Space: An Invitation to the Table of Negotiations”[[3]](#footnote-3). Yet, we were not the first ones to embrace such a complex endeavor. At the United Nations, Russia has as of 1998, in a series of UN draft resolutions, advocated a Cyber Treaty, proposing detailed, although conflictual and probably unimplementable contents[[4]](#footnote-4). These draft resolutions became an annual exercise in frustration: the Russian initiative was for many years rejected by a number of Western countries, but yet had the undoubted merit of keeping the argument alive that a major normative effort was required.[[5]](#footnote-5) ITU Secretary General Hamadoun Touré has early on, and then repeatedly, called for a “Global Cyber Treaty”[[6]](#footnote-6), laying out some essential provisions. He has thus added an authoritative UN voice to the quest for a normative framework. Many other advocates for comprehensive treaty-making could be cited[[7]](#footnote-7).

But however attractive the concept of a comprehensive Convention on Cyber Space – comparable to the UN Convention on the Law of the Sea of 1982 - , the obstacles to such an instrument and its creation were increasingly recognized as overwhelming. Cyberspace might be even more complex than the ocean world. Digital technologies and their uses are still evolving at a rapid pace. Universal treaty-making would be beset by still bigger cleavages in individual nations’ views. Treaty negotiation would be a lengthy process, and national ratification procedures would not proceed on a time scale even marginally in keeping with the urgency to fill the legal void and the growing, shared perception among governments that the threat of cyberconflict and unmanageable cyber damage is escalating out of control. Binding commitments to avoid attack or hostile actions and corresponding sanctions would be unworkable. Important definitional issues would probably be unresolvable in treaty language. Thus, while a Universal Treaty/Law on Cyberspace remains a preferred objective, a target concept, practical reasons require an alternative approach.

If a one-shot cyber treaty thus is not a realistic option, or is not timely – or if early concentration on the treaty idea was perhaps even a wrong start - , neither does a simple extension by analogy of the laws of armed conflict or humanitarian international law into cyberspace do the trick. There are areas of ambiguity, including the scale and nature of damage from cyber attack that could qualify as use of force which, in a rapidly evolving digital environment, would defy treaty-making or treaty analogies.

Fortunately, collective thinking about the necessary processes of cyber strategy has notably evolved. To make a long story short, a new age of cyber diplomacy has begun around 2008 with a manifestly emerging international consensus to concentrate efforts on an alternative to formal treaty-making: the elaboration of confidence-building measures or codes of conduct as normative tools. We may be witnessing a turning point in cybersecurity diplomacy.

Both of them, CBMs and codes, are time-honored techniques of international diplomacy. Confidence-building measures have been a major focus in reshaping the East-West relationship in the CSCE/OSCE and in military affairs elsewhere, including in the United Nations context (taking their methodological guidance in particular from the outcome of the OSCE process, but also from the Guidelines for Confidence-Building Measures adopted by the UN General Assembly in 1986[[8]](#footnote-8)), and codes of conduct are constructed in many other areas of the social environment including the private sector. In the UN, there have been negotiations on a code of conduct for the transfer of technology, and a code of conduct of behavior in Outer Space is presently in process[[9]](#footnote-9). In our context, the two methods are frequently mentioned together, and indeed, they may be somewhat interchangeable: both aim at regulating behavior; CBMs look more to the intended result, the term code of conduct reflects the notion that an ample, coherent body of norms is being negotiated[[10]](#footnote-10).

The prevailing view is now that CBMs open a window of opportunity to make real progress towards common definitions and behavioral standards. CBMs have the potential to reduce threat, enhance transparency, make State behavior predictable, are flexible, voluntary, and offer a variable geometry in terms of participants – it is possible to include non-State actors - and follow-up: contrary to coherent treaty-making, participants are free to adopt partial solutions and enact them without delay and independently or with other like-minded stake-holders. CBMs which States embrace do not require ratification; they invite emulation, and are at most – and at best - politically binding. They are thus uniquely suited to foment international consensus-building on an evolutionary scale. A well negotiated package of CBMs with a critical mass of participants may set in motion a process of further incremental change and heightened sensitivity. Clarification of behavioral standards may provide an incentive for going for more.

One catalyst for this new campaign may well have been the terse report of the second UN Group of Governmental Experts 2010[[11]](#footnote-11) (the first having ended inconclusively) recommending further international discussion on norms, confidence-building, stability and risk reduction measures. A natural result was the convocation of a third GGE, this time with the concrete mandate to define “cooperative measures . . including norms, rules of principles of responsible behaviour of States and confidence-building measures with regard to information space”[[12]](#footnote-12). The Group will convene in August, coinciding in time with this Seminar, under the presidency of an Australian diplomat. Governments have provided numerous inputs to the Group at the request of the UN Secretary General[[13]](#footnote-13). Their views have strongly supported the idea of identifying CBMs. In a short time, flurries of other national statements to the same effect have surfaced: from Australia, the UK, Germany, at least by implication the US, among others[[14]](#footnote-14). An authoritative academic voice from India has joined the concert[[15]](#footnote-15). China, Russia, Tajikistan and Uzbekistan, reflecting work within the Shanghai Cooperation Council, submitted to the UN Secretary General, in September 2011, a draft international code of conduct for information security[[16]](#footnote-16). Although the document, by virtue of its choice of authors, did not seem to display a sufficient flavor of political correctness, the catalogue of commitments, offered for voluntary subscription by States, should not be disdained. In the meantime, member countries have organized prestigious international conferences, where the CBM idea has been ventilated, and more or less detailed catalogues of CBM contents have figured in the Conference summaries (London[[17]](#footnote-17), Berlin[[18]](#footnote-18), Beijing, Viena[[19]](#footnote-19), with other conferences forthcoming in Budapest in October 2012 and South Korea in 2013). Apart from the on-going UN exercise, regional organizations are also getting into the act. The ASEAN Regional Forum with its representative membership and participants, 27 nations going much beyond Asia, has zoomed in in full on the CBM theme[[20]](#footnote-20). The OSCE, mindful of its earlier experience with East-West CBMs, is intensively working on a draft code of conduct (see “A Comprehensive Approach to Cyber Security”)[[21]](#footnote-21) and APEC[[22]](#footnote-22), as well as the aforementioned Shanghai Cooperation Organization[[23]](#footnote-23) are also working on regional arrangements. The Council of Europe, famous for its contribution to a world penal law on cyber crime through the Convention on Cybercrime, has adopted 10 Principles on Internet Governance[[24]](#footnote-24). UNIDIR helps to provide the academic underpinning for these endeavors[[25]](#footnote-25). ONGs in the cyber area, as the ICT4Peace[[26]](#footnote-26), or individual researchers like the Estonian scientist Eneken Tikk[[27]](#footnote-27), provide catalogues of rules of conduct of their own. These catalogues can obviously not be reproduced or analyzed here – I will revert to the task waiting for us there – but provide effective tools for spurring the debate and facilitating CBM negotiations. I hardly need to remind you that our own Erice Declaration on Principles for Cyber Stability and Cyber Peace of August 2009[[28]](#footnote-28) also urges a common code for cyber conduct.

Just to give the audience the flavor of where codes of conduct may lead us, I will provide subsequently an indicative list of important provisos which CBMs or a code of conduct negotiation should consider. The list comprises the tenets I personally have been working with, but also reflect the principles Secretary Hamadoun Touré and the ITU consider essential, and some ideas from other catalogues. The list is not only indicative, but also very general, as CBM negotiations, other than treaty-making, only lend themselves to very basic commitments.

The list would read as follows:

Binding agreement on the fundamental principle that a cyber attack against another State, direct or through hired perpetrators, constitutes a violation of international law.

Commitment of all States not to practice first use of cyber weapons against another State, as long it has not already undergone an attack by conventional weapons.

States subscribe, nationally and internationally, to a policy of prevention of cyber conflicts, placing the emphasis on cyber defense, and will therefore, jointly with the private sector, secure their systems and networks through maximum robustness and potential of resilience, built-in redundancies, net segmentation, “cyber higiene”, efficient management, and similar measures. States will to that effect collaborate in international standard-setting.

In case of a cyber attack or grave disturbance of their net structures in process, States will aim at the restoration of intact networks and of stable peaceful communication structures at the earliest point in time.

States are responsible for the protection of critical infrastructures on their national territory, particularly of those ensuring energy availability, banking services, public health, and installations serving other humanitarian purposes, and to ensure the inviolability of transnational digital net structures. Attacks on these structures are prohibited.

States are obliged, in the interest of a uniform or harmonized international protective legal framework, to introduce comprehensive penal legislation for the persecution of cyber crime – be it by adhering to the Convention of Cybercrime of the Council of Europe, or by adopting comparably comprehensive arrangements – and to ensure the efficiency of law enforcement and the requisite international cooperation for that purpose.

States have the duty to protect their national citizens in cyberspace.

States must not tolerate cyber terrorists or cyber criminals operating in or from their territory without due punishment. States are obliged, within available technological means (for example, through deep packet inspection of the principal fiber circuits of their ISPs) to impede and reveal the use of their territory by cyber criminals.

The use of botnets and other irregular cyber war practices is forbidden, and States are obliged to implement this prohibition on their national territory.

Neutrality continues to be valid in the cyber age, and cyber attacks must not be perpetrated through the net structures of neutral States.

States must commit themselves to mutual assistance in the reconnaissance and detection of cyber crimes, particularly if the attack has issued from their territory. States are to participate fully in the existing information and early warning systems, by adhering to the agreements on 24/7 contact points and international CERT networks, among others.

States are invited to conclude, in addition to multilateral agreements, bilateral accords containing reciprocal non-aggression commitments, arrangements for the joint defense against cyber attacks, and mutual assistance in case of damage inflicted. Unilateral declarations aimed at renouncing any cyber activity that might cause large-scale harm to civilian critical infrastructures are also desirable.

States will ensure an open Internet that allows individuals access to content and services with only such restrictions as are permitted under international legal obligations, while protecting users against abuse, especially children. Government restrictions on the freedom of the Internet will be duly incorporated into law and subject to independent judicial review.

That such catalogues of suggestions for future norm-making now appear realistic is certainly a welcome development. Yet, the road ahead is far from clear or without obstacles. Current activities in the field of cyber diplomacy take place in an environment of prevailing deep distrust, high secrecy especially as regards military cyber applications, wide disparities of views among States, insufficient research on important regulatory issues, and lack of a common vision of how a future order of cyberspace would look: most of the suggested lists are unsorted, with unclear overlaps. Some crucial issues may not lend themselves to a CBM negotiation on broad principles at all: many definitions, detailed rule-making on what constitutes “armed attack” or what responses would be justified, what rules of engagement should prevail, etc. would probably need long-drawn supplementary negotiations, to be outsourced to specialized bodies. (NATO and some governments like the US are already working on these issues). Important as general principles are, this may well prove to be the most difficult part.

Then there is the general question of venue. Where should negotiations on CBMs or codes be located? (I will revert to that issue). What are the ground rules to be? Will participation be inclusive, allowing stakeholders other than States, to join? The need to practice a multi-stakeholders approach in Internet Governance is now generally recognized and must be translated into procedural reality. If there are to be several parallel negotiations, for instance by regional international organizations – the OSZE, APEC, the Shanghai group, NATO – how can the results be synthesized to generate uniform rules and a combined impact? As no one universal draft treaty is aimed at, and involvement is voluntary, participants should agree that each one has the right to pick individual measures or code elements and enact them early and separately; there must not necessarily be packages. Could there, then, be a sequence of stages? What would be the time frame?

What we see at the present juncture is no more than work in progress. As it shapes up, problems of structure and content will constantly emerge. They need to be identified and researched. This is where contributions from outside, including the academic community and dedicated NGOs need to come into play, to accompany and help shape the process. I see a definite role for our PMP. In our work we can contribute to a stock-taking of the multiple efforts presently under way, make an independent assessment of the ideas proffered by Governments and explore their consensus potential. It may sound ambitious, but this may be the opportune moment for a cool, objective assessment of each stage of the evolving process, and for helping to put matters into a coherent and clear focus. A group as ours can help to prioritize the various planks of the negotiation, to make for more transparency in the underlying doctrines, and to press toward better mechanisms of international cooperation and crisis management. We may also be able to make a well-reflected input into the pending issues of developing international law for the requirements of the cyber age, as we have already begun to do in several of our documents. In short, a creative input of the PMP could be a very apposite contribution in furtherance of our concept of cyberpeace.

An issue, already touched upon and needing penetrating thought, and also discussion within our Group, is the identification of an optimum venue to host the (hopefully) forthcoming negotiations on CBMs or Codes of Conduct. I do not want to preempt that debate, but from the universal perspective of our PMP, a single forum offering such universal perspective would certainly be the most adequate. On the other hand, preliminary regional endeavors are already under way, and their dynamics should be used. The OSCE, although it has no recent treaty-negotiating record, has the advantage of comprising States on the East-West axis, some of which have distinct cybersecurity problems. Confidence is particularly needed in such environment. If a regional approach prevails, some coordinating mechanism should be developed to avoid contrasting or contradictory standard-setting. If one wishes to avoid the heavy UN machinery, an autonomous Conference of States, perhaps serviced by the UN, would be a good bet. I have never hidden my preference for the ITU as the principal venue and coordinating instance in the cybersecurity domain[[29]](#footnote-29). But in other contexts I have also thrown out the idea of entrusting the Conference on Disarmament with its perennial negotiating experience in the security domain[[30]](#footnote-30). And has anybody probed the suitability of the Council of Europe, its relative geographical limitation notwwithstanding? The political implications and acceptance potential of any of these options have to be weighed carefully, and experts on international machinery are invited to provide their input.

1. Chairman, Permanent Monitoring Panel on Information Security, World Federation of Scientists, Ambassador of Germany (ret.). Presentation given at the 45th Session of the International Seminars on Planetary Emergencies, Erice, Sicily, 22 August 2012 [↑](#footnote-ref-1)
2. Document WSIS-03/GENEVA/CONTR/6-E,, [www.itu.int/dms\_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006%21%21PDF-E.pdf),, also at www.unibw.de/infosecur [↑](#footnote-ref-2)
3. UNITAR, Geneva 2005, www.in.int/kamal/the\_law\_of\_cyber\_space [↑](#footnote-ref-3)
4. Res. A/53/70, annually up to A/65/41. The Russian initiative has for many years benefitted from the leadership of a member of our PMP, Ambassador Andreij Krutskih [↑](#footnote-ref-4)
5. The need for a normative effort is now universally acknowledged. Examples: Michael A. Mazarr “Rivalry’s New Face”, SURVIVAL, vol. 54, August-September 2012, p. 100: “A key priority should be building norms, agreements and institutions that keep various agents locked into stable habits”. And the search for formats to foment norm-building was also a recurrent theme in the cyber session of the Shangri-La Dialogue, IISS news, July 2012. [↑](#footnote-ref-5)
6. “UN Chief proposes int’l accord to prevent cyber war,” 31 Jan. 2010,

www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a. [↑](#footnote-ref-6)
7. The Federation of Russia has, in 2011, developed a new draft for a comprehensive treaty, although apparently it has not been officially submitted to the UN ([http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/6912ce36aa5f1e92c32579250035bebd!OpenDocument](http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/6912ce36aa5f1e92c32579250035bebd%21OpenDocument))
 [↑](#footnote-ref-7)
8. Reprinted in UN document A/S-15/3. For the development of the concept in Europe and beyond see Henning Wegener “CBMs: European and Global Dimensions” in: F. Stephen Larrabee and Dietrich Stobbe, eds., “Confidence-Building Measures in Europe”, Institute for East-West Studies, New York, 1983 [↑](#footnote-ref-8)
9. See also the Montreux Document on Operations of Private Military and Security Companies During Armed Conflict, www.icrc.org [↑](#footnote-ref-9)
10. Some governments, including the Federal German Government, prefer the term Transparency- und Confidence-Building Measures (TCBMs). As the promotion of transparency has always been a major plank of CBMs, the choice between the terms would seem to be one of emphasis rather than substance [↑](#footnote-ref-10)
11. A/65/201 [↑](#footnote-ref-11)
12. A/Res/66/24 of 13 December 2011 [↑](#footnote-ref-12)
13. A/66/152 and A/66/152 Add.1 [↑](#footnote-ref-13)
14. See previous footnote and the positive utterances at the cyber session of the Shangri-La Dialogue, IISS news July 2012. For Germany, see also “Challenges in Cyber Security: Risks, Strategies and Conference Building, Conference Report, December 13 and 14, 2011, Berlin, [http://www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/ Abruestung/Projekte/ Cybersicherheit.html](http://www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/%20Abruestung/Projekte/%20Cybersicherheit.html).The German Federal Foreign Office, in addition, supports a 2012 UNIDIR project on International Cybersecurity and CBMs [↑](#footnote-ref-14)
15. Arvind Gupta, CBMs in Cyber Space: What Should Be India’s Approach?, IDSA, Institute for Defence Studies and Analysis, June 27, 2012 [↑](#footnote-ref-15)
16. A/66/359. See also the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, signed in Yekaterinburg on 15 June 2009 [↑](#footnote-ref-16)
17. See www.fco.gov.uk/en/global-issues/london-conference-cyberspace/ [↑](#footnote-ref-17)
18. See footnote 9 [↑](#footnote-ref-18)
19. An OSCE Conference, May 9 and 10, 2012 [↑](#footnote-ref-19)
20. Secretary of State Clinton at the Pnom Penh ASEAN meeting on July 12, 2012: “This Forum includes some of the world’s largest cyber actors. So this is an appropriate setting for a sustained, meaningful dialogue on cyberspace issues. In the years ahead, we should work together in support of responsible norms and standards, and pursue practical measures to build confidence and reduce risk”. The ARF organizes a Seminar on Confidence-Building Measures in Cyberspace in Seoul next September. In May of this year ASEAN defense ministers called for an ASEAN “master plan of security connectivity”. [↑](#footnote-ref-20)
21. 21 www.osce.org [↑](#footnote-ref-21)
22. See the APEC TEL Strategic Action Plan 2010-2015, www.apec.org [↑](#footnote-ref-22)
23. No home page in English of the SCO could be detected. News are best gathered from the web pages of the member countries. [↑](#footnote-ref-23)
24. hub.coe.int [↑](#footnote-ref-24)
25. UNIDIR organizes conferences and participates in others. See also the articles in DIARMAMENT FORUM [↑](#footnote-ref-25)
26. http://ict4peace.org [↑](#footnote-ref-26)
27. “Ten Rules for Cyber Security”, SURVIVAL vol.53 no.3, June-July 2011 [↑](#footnote-ref-27)
28. Reprinted in “The Quest for Cyber Peace” www.itu.int/S-GEN/WFS,01-2011-PDF-E, , p.110 [↑](#footnote-ref-28)
29. Henning Wegener, “Harnessing the perils in cyberspace: who is in charge?” UNIDIR, DISARMAMENT FORUM 3/2007. Indubitably, the ITU possesses the technical expertise, political perspective, organizational capacity and negotiating experience to handle such a task, However, a number of countries wish to deemphasize the political relevance of ITU and – erroneously – consider it a merely technical service organization. [↑](#footnote-ref-29)
30. My views have no doubt been shaped by personal experience, representing my own country at the CD more than five years. [↑](#footnote-ref-30)