**International Conference on Cyberlaw, Cybercrime & Cyber Security**

New Delhi, November 19, 2015

**Norm-Making in Cyberspace: the UN contribution, - slow and incremental, but essential**

**Ambassador Henning Wegener**

**Chairman, Permanent Monitoring Panel on Information Security, World Federation of Scientists**

I feel privileged to be invited again – for the third time – to this important series of conferences on the most topical and ardent issues of the cyber age. As in the previous instances, apart from being here myself, I also represent the World Federation of Scientists, being the Chairman of its permanent observatory on cybersecurity. I am happy to remind you that Mr. Paval Duggal, the *spiritus rector* of this conference is also a member of that world-wide group.

Everyone has his preferred subject. Mine, and that of my group, is the concern with the normative order of cyberspace in a universal perspective, convinced that a globally effective technology with global benefits and risks – especially the latter – needs global legal frameworks. Today I propose to offer yet another variation on that theme which I already treated on the two preceding occasions Recalling my earlier presentations I do not intend to repeat myself, - self-plagiarizing is not a very noble trade. Instead I will merely make reference to the sites where the earlier papers can be found, if anybody has a deepened interest in the subject matter. However, my main purpose is to demonstrate how we have been proceeding apace in what last time I called the emerging era of world cyber diplomacy, what recent developments are, and where we should move from here. If last year I provided a synthesis of international cyber activities, this time I plan to demonstrate the current state-of-the-art of one major strand of international negotiation that takes place at the United Nations. I refer to the successive sessions of the Governmental Groups of Experts on International Security in the ICT field.

Before I sum up the history and importance of this UN activity let me underline the growing urgency of decisive normative steps in the digital world. Cyberspace is becoming an ever more dangerous space. 2013 may have been the break-through year from which onward almost all indicators of cybercrime and cyberconflict have demonstrated exponential growth rates. They have continued to create instability and geopolitical tensions. The dramatic rise in digital devices – most of them vulnerable to cyber attacks -, the growing all-pervasiveness of IT in the operation and steering of economic and social structures, an invasion into almost every precinct of human and societal endeavor, the corresponding speed at which malicious ICT agents are multiplying and spreading, and malicious actions are undertaken, the enforced speed at which States – and non-State actors – are developing ICT capabilities for military or other bellicose purposes, - the list of ominous developments is long, and has been illuminated in its many facets in this conference.

Before the menacing background of this new threat landscape, we observe a major increase in the quest for comprehensive norms and legal frameworks that can stem dangerous tides and fill the still blatant void in the management of the cyber age. However, the emphasis has changed along with the volume of activities.

Early collective efforts had been directed at building a comprehensive Convention on Cyber Space – comparable to the UN Convention on the Law of the Sea of 1982 - through a UN process as its monopoly wielder. However, 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 at the UN 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 and important definitional issues would probably be irresolvable in treaty language. Thus, while a Universal Treaty/Law on Cyberspace must remain a preferred objective, a target concept, practical reasons require an alternative approach.

If a one-shot cyber treaty thus does not prove a realistic option, 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 evolved since then. 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 for the responsible behavior of States as normative tools. Both techniques, CBMs and codes, are useful – and at that mutually complementary instruments for advancing normative processes.

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 stakeholders. 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. Codes of conduct may achieve responsible cyber behavior by States by acceptance also as voluntary guidelines, but would unfold their regulatory effect even more strongly if negotiated into binding prescription. Such codes, if agreed, are especially significant.

With such insights, CBMS and codes of conduct have become over the last few years the center of the new era of cyber diplomacy. And its key features are diversity and multiplicity of actors. Along with the omnipresence of the digital culture, arrived the concept of “multistakeholding” in its management, and in the elaboration of norms. While norms for responsible cyber behavior of nation-States, and their norm-setting role nationally and internationally are indispensable given their primary responsibility for maintaining a secure and peaceful IT environment, it has become increasingly clear that groups of nations, international organizations, digital industry/the private sector and societal institutions also have their contribution to make and to help knit the normative fabric of a universal order of cyberspace. There is now a creative burst of attempts at norm-setting, with the code of conduct idea being given concrete shape by the G8, the OSCE, the EU, APEC, NATO, the Shanghai Cooperation Organization, and many others.

Many of these deliberations have recently been reflected in the negotiation strand which I would particularly like to emphasize: the successive convocation at the UN of Governmental Groups of Experts with a broad brief to deal with the principal normative issues. The 4th one of these groups has concluded its work this summer, and the conclusions contained in its report to the UNGA, through the Secretary General, A/70/174, have been taken note of approvingly by the First Committee in a UNGA resolution, A/C.1/70/L.45 only a few days ago without a vote, which is to say, unanimously.

The report produced by the “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, - thus the complicated denomination – of 2015, as appears from its numbering, is not a stand-alone product. The Group’s work, and its mandate “to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behavior of States and confidence-building measures with regard to information space, as well as the concepts aimed at strengthening the security of global information and telecommunication systems”, takes off from the results of its predecessor, the (2nd) GGE and its report of July 2010 (A/65/201), as well as the 3rd one of 2013, A/68/98, and also benefits from the trends set in motion by a serious of Government-sponsored multi-stakeholder conferences from London to Seoul and The Hague, where the very discussion on norms and confidence-building reflected in the GGE’s mandate took center stage. The many consultation processes in regional organizations, and major international organizations which I mentioned before also provided intellectual inputs, so that the GGE Report reproduces evolving common perspectives, and in some instances emerging consensus. It stands in a continuity of mature reflection about the cyber issues on hand. At the same time, it marks a new step in that problems already under discussion elsewhere are synthesized in a new way, by a representative, quasi global group of Governments. Also, the continuation of the process is assured by the creation of a, further (5th) GGE with an equally broad, representative membership for continued study of the recommendations of the Report (A/RES/70/174). This continuation of the process carries a momentum that offers the promise for further stages of global consensus.

What do we have to retain from the Group that has reported out in 2015? The work, after an initial threat analysis, is subdivided in three parts, norms, rules and principles for the responsible behavior of States, confidence-building measures, and international cooperation and assistance in ICT security and capacity-building, the two latter overlapping to some extent; the structure of the reports of the preceding groups has thus been maintained. And as perhaps the most important result one should retain; the applicability of international law in all its facets to the digital space has not only be confirmed, but stated in more detail, and that by a larger, and more representative group of governmental representatives. This confirmation also figures clearly in the recent UNGA resolution adopting the report, and establishing the follow-on GGE. Beneath that level, if one goes over the two last reports paragraph by paragraph, the results are very similar. The legal obligations spelled out on the basis of the basic confirmation of the applicability of International law in all its facets often differ only in wording, but regulate the same subject matter. However, the recent catalogue is more extensive and more concrete. Among the international law tenets, the validity and full respect of human rights on the Internet, the right to privacy and the right to freedom of expression are now clearly spelled out – important norms in the face of the sadly growing Internet censorship in many countries. The international protection of critical national infrastructures, the common fight against terrorism and States’ obligations in this respect, the obligation to curtail and pursue malicious ICT activities in the State’s territory, the protection of national emergency response teams, - these and other important issues have been addressed more straightforwardly.

On the whole, the GGE report shows continuity, but also real progress, and the level of international consensus on the whole outcome has certainly increased.

However, lest too euphoric a view prevail, a major *caveat* is in order. Although a wider-ranging verbal consensus among the Group – and impliedly by their governments – has been achieved, and international approval and support have been gathered, the basic ambiguity between the principles endorsed – mostly couched in familiar Charter and International Covenants terms - for instance between universal positions and State sovereignty and sovereign equality, remains unresolved and is apparent in many portions of the text, especially those relating to the jurisdiction over ICT infrastructures, inherent States’ rights to take measures, human rights, and freedom of expression in the digital sphere. These ambiguities are of course age-old, but they are of particular relevance in the quest for a universal normative management of a globally effective technology that negates space and time, and makes the “territorial integrity” and even the total political independence of nation States concepts that can no longer be taken as absolutes. Behind the emphasis on governmental superiority looms the specter of a government-run Internet and control of both users and content. The question to what extent *doublespeak* is at work here comes to mind especially when one looks at the sponsorship of a draft International Code of conduct for information security by the governments of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan (A/66/359, in its second version, A/69/723), cited by the GGE, piously couched in traditional, universalist UN language, but with a clear bias towards unconstrained national action, even vis-à-vis clear international commitments. And questions also arise when the 25 sponsors of the already mentioned UN resolution that approves of the report of the 4th GGE and sets in place its successor 5th group exhorts all Member States to be guided by the recommendations of the 4th Group – including the right of freedom of expression, while Freedom House has characterized more than half of these sponsors as countries “not free” or only “partly free”, practicing wide-ranging Internet censorship. The profound ambiguity I have alluded to – which is, in fact, a deep ideological rift – has also in the past characterized the debates on Internet Governance, where, however, the constructive consensus language of the NetMundial Multistakeholder Statement document adopted by a world conference in Brazil in 2014 has given hope that a gradual *rapprochement* of positions can be attained.

The same hopeful perspective should govern the future two-year work span of the 5th GGE. Its mandate, almost identical with that of its predecessor, asks the Group to “continue to study” its subject “with a view to promoting common understandings”. The prescribed path is thus to narrow the ideological differences, - and to be more concrete Ambiguity grows with generality. As the great achievement so far is that consensus has been achieved on much of the language, in great part hallowed language from universal UN documents which carry with them the age-old support of a large majority of nations, it would appear difficult to go against their message and spirit. A more detailed examination of the problems in a case-per-case mode can be conducive to more consensus and circumscribe ambiguity, closing escape hatches. The basic agreement that international law, and in particular the UN Charter, is applicable to cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful an accessible ICT environment, is a common basis for further progress and not to be underestimated. The accord that existing international law – where it is uncontroversial – both below and above the threshold of the law on armed conflict – can be supplemented by non-binding norms that define and shape expectations has the propensity to foment responsible State behavior. The same holds for the acceptance of the International Covenants on Human Rights and the principal instruments of humanitarian law, the rulings of the Human Rights Council on freedom of expression and most of the norms, measures and principles enumerated by the latest GGE. Further detailed work, the *first*  task of the GGE, is thus likely to be healthy and to generate at least incremental further progress.

However, the focus of the normative effort should be broadened. I would suggest as a *second* task of the new group that it also studies State obligations like the following, not yet addressed: Commitments not to practice ICT means of attack first, unless there has been a clear military conventional attack; an obligation of States to endow themselves with comprehensive penal legislation and efficient law enforcement against illegal ICT use; a legal guarantee of the protection of national citizens in cyberspace; the interdiction of botnets; an obligation to ensure by law that restrictions on Internet freedom are regulated by law and only under judicial review. Finally, the GGE should also ensure that the neutrality of States continue to be valid.

Another – *third* - important task of the recently created GGE would be to develop a concept how the manifold normative endeavors of regional international organizations and other multistakeholder actors could be integrated into a more comprehensive, single normative order, - at least in the sense of harmonious interaction and mutual compatibility among the various stakeholders. That also implies a reinforced thought process on future negotiation processes. Somebody should pull all these diverse, but similar strands of norm-making together! It would be worthwhile to compare and analyze these various drafting efforts, extract their common substance with a view to a synthesis, organize the interplay between international and national legislation, and to use this exercise to foment universal norm generation. The time for convergence has arrived.

This leads to what I see as a *fourth* implied assignment for the 5th GGE: finding a venue and a calendar for a true negotiation. The UN cannot go on indefinitely with merely studying the norms we need. An ever more refined study will be useful and will certainly heighten consensus, but even norms that are designed as voluntary need a point of fixation, and operative indices for adoption and implementation. The process needs to be lifted from the level of Government Experts to that of Governments. Many options for a negotiation setting have been tossed about in recent times. My preferred solution would be a UN-sponsored Conference of States that, however, beyond government delegations, would also allow other multistakeholder representatives, including the private sector and civil society, to participate and to share in any emerging consensus. There is precedent for such a mix of States and non-State interests. In a UN framework, unity of purpose, primacy of a universal perspective, and overall cohesion are best attained. The search for an over-arching negotiation strategy is urgent and should be pursued vigorously in the new GGE format.

If the processes here described are to serve as an important tool in the gradual establishment of a universal order of cyberspace, even a tool of growing relevance, it is legitimate to inquire what role India is to assume in this process. India as one of the most advanced nations in digital technology, a primary force in the world software industry, with an exemplary national legislation on cyber matters since the IT Act of the year 2000, is also on its way to become the first economic world power in the very near decades, surpassing China and the US, thus also leading the digital world. Yet I am afraid to say that the Indian Government so far has not played an outstanding role in the multilateral processes under discussion. India has, to my knowledge, never co-sponsored a UN resolution in this field, has been present in only one of the GGEs, and been absent in the most important one, the 4th; the country has to my awareness never joined other nations in honoring the Secretary General’s invitation to provide to him annual assessments on issues of information security, as a basis for the work of the Experts. Nor has India adhered to the International Convention on Cybercrime, a key document in establishing a universal format for persecuting cyber crime and collaborating on a treaty level in world-wide cyber law enforcement, even though this very month additional relevant countries like Sri Lanka or Canada have swelled the ranks of treaty members. Global cyber space conferences have lately advanced the multilateral process – the cycle initiated by London now includes Berlin, Budapest, Seoul, lately The Hague, and soon Mexico - but India has not yet chosen to be a host at such world event despite her eminent qualifications. I hope to be not too daring in suggesting that the country’s role in international cyber diplomacy might warrant another look. The idea of an International Commission on Cybersecurity Law pioneered by the Chairman, Mr. Duggal, could be an important step in this direction.

**Amb. Henning Wegener – Earlier articles and presentations**

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

Presentation at the 45th Session of the International Seminar on Nuclear War and Planetary Emergencies, 2012, Yearbook, The Science and Culture Series, World Scientific Publishing Co, Sinapore2013

**Maintaining Cyber Peace, Restoring Cyber Confidence** Conference on Cyber Law &Cyber Crime, New Delhi, March 2013

**UN and Member States’ Approach to Internet Norms, Rules and Principles: Evaluation of the Report of the UN Group of Governmental Experts**

In: The Quest for Cyber Confidenceby Dr. Hamadoun I. Touré and the Permanent Monitoring Panel on Information Security, World Federation of Scientists, [www.itu.int/publications](http://www.itu.int/publications), 2014

**A New Era of Cyber Diplomacy: In Search of Comprehensive International Regulatory Frameworks**

International Conference on Cyberlaw, Cybercrime & Cyber Security, New Delhi, November 20, 2014

All the foregoing are also available at www.unibw.de/infosecur

**Reports of UN Government Groups of Experts – UN documents**

**2nd GGE: A/65/201**

**3rd GGE: A /68/98**

**4th GGE: A/70/174**