**Conference on Cyber Law & Cyber Crime**

**New Delhi, March 13, 2014**

**Maintaining Cyber Peace, Restoring Cyber Confidence**

***Henning Wegener***

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

It is a privilege to be invited to this Conference; and indeed a double privilege, as the Cyber group I chair in Europe has at the same time been asked to be a co-sponsor of this event. You have heard me reading out a message from Professor Antonino Zichichi, the President of the World Federation of Scientists. He has referred in a nutshell format to one of the important activities of the Federation, its quest for Cybersecurity. While I now make my own remarks, let me revert to, and paraphrase some of the things he had to say on our calling in the cyber sphere, before I raise some specific points.

You have heard that the WFS has started out, so many decades ago, motivated by concerns over the perils of the nuclear age, and that its central purpose, pursued by some of the brightest minds of the time, has been to stave off the dangers, and heighten the benefits of this frighteningly ambiguous technology, nuclear technology. Since its focus has broadened to encompass a range of emergencies that hail from other ambivalent technologies: ambivalence may well be the hallmark of men’s venturing out into new technological domains. In 2001, I had the good luck to be able to assist in the creation of our cyber security group, and have since been its chairman.

It is not that cyber insecurity, the emergence of cyber crime and the specter of cyber military conflict were then new. In many quarters they were already a matter of high concern, and much excellent work had been accomplished in the nineties of last century by farsighted governments and individuals. I was reminded by other speakers that the Indian IT Act was adopted as early as 2000, a trail blazer indeed. Yet the situation then, however problematic it appeared at the time, pales in comparison with the challenges we face now.

In the process I think the World Federation of Scientists has to some extent broken new ground. In the few years since its inception, cyber technology has come to form the dominant paradigm for the functioning of all segments of our societies, and the then unimaginable universal growth of digital devices has come along with universal interconnectivities of exponential scale and an even steeper curve of exponentiality as regards risks and vulnerabilities.

Lodging our monitoring group within the World Federation has from the beginning given us the fertile multidisciplinary environment needed for a conceptual approach to cybersecurity and the appreciation of the new dangers.

It is also a geographically diversified environment. Let me cite the names of some of the members of our cybersecurity group: Robert Kahn, one of the legendary fathers of the Internet; Hamadoun Touré, Secretary General of the ITU; Ambassador Gábor Iklódy, long-time Assistant Secretary General of NATO for Emerging Security Challenges; Professor Howard Schmidt, the former Cybersecurity Coordinator, “Cyber Czar”, at the Obama White House; Udo Helmbrecht, Executive Director of the European Union Agency for Network and Information Security, ENISA; Mohd. Noor Amin, the Chairman of IMPACT, the International Multilateral Partnership Against Cyber Threats; Ambassador-at-Large Andrey Krutskih, since many years the Russian spokesman for cyber security in the UN. And from India, of course, since last year, our host, President Pavan Duggal. We are all happy to be able to count on his experience and vision.

As already prefigured in Professor Zichichi’s slides, our group has from the outset been less concerned with the technicalities of cyber protection, rather we have tried to make a contribution to the overriding issues of ordering cyberspace and make it a peaceful, stable, legally regulated environment. Managing cyber conflict has been our major emphasis. We have always believed that starting from a broad analysis and grasp of the underlying technological realities, working on the more conceptual perspectives is essential

Our first comprehensive document, drafted in 2001 characteristically read: “Toward a Universal Order of Cyberspace. Managing the Threat from Cyber Crime to Cyber War”. In an amended version we introduced it as a conference document at the first phase of the World Summit on the Information Society in 2003. From later documents, suffice it to cite our very conceptual document of 2009, the “Erice Declaration on Principles for Stability and Cyber Peace”.

Cyber Peace has continued to be an important orientation in our work. The starting point has been our increasing concern about offensive military uses of digital technologies, unbridled by accepted codes of conduct, but also our analysis that cyber war is not only an elusive concept, very difficult to define or to delimit, - digital attacks on systems and cyber infrastructures hit military and non-military targets alike . – but that any attack on the now all-pervasive net structures affects (all) digital effects that defy borders and societal segments. Worse, the very notion of cyber*warfare* is conducive to stimulating military thinking patterns and analogies from conventional war with possibly perilous consequences. Cyber Peace stands in deliberate contrast to the negative phenomena of cybe rwar, cyberterrorism and cybercrime. To opt for the positive side in the war-peace antinomy implies an important change in perspective and scale of priorities, as it orients the mind towards the benefits and positive potential of the Information Society and provides a goal post to that effect, reinforcing the negative connotation of cyberwar and related terms and calamities, and fomenting dynamic movement towards a global culture of cyber security. This attempt to delegitimize cyber war through reversing the perspective is fully aware that digital infrastructures are now all-pervasive, and will unavoidably also be used for hostile purposes. The over-riding objective, then, is to harness them and provide the strictest possible limits for their application. We have attempted to define the peace concept in “The Quest for Cyber Peace” a book written jointly with Secretary General Touré and published in 2011 as a UN publication.

Our approach and the term cyber peace have been picked up in many other quarters. Those interested in our work may refer to our web page [www.unibw.de/infosecur](http://www.unibw.de/infosecur) where they find numerous recent writings that flesh out our basic conceptual tenets.

Another basic concept on which we concentrate is “cyber confidence”. Trust, confidence is a clear prerequisite for a functioning digital society that is to generate the expected benefits. An open, global, accessible and secure cyberspace that respects the right to free information and privacy reposes on such confidence. Confidence is the red threat that runs through every attempt to create a harmonized legal and normative framework to combat cyber crime and cyber conflict.

Yet, it is no exaggeration to say that there is now a crisis of cyber confidence. There are several causes for this critical development.

* Growing concerns that cyberspace is becoming militarized and that ever more States are developing offensive military capabilities directed at the adversary’s infrastructures, with uncontrollable overspill effects, and no inhibitions slowing a digital arms race
* Increasing anxieties that civilian infrastructures of vital significance will be attacked by States or non-state actors,
* An ever more complex technical environment with great potential, but also new vulnerabilities and unpredictable consequences for a universe of interconnectivities.
* The emergence of uninhibited, limitless and technically unharnessed intrusion into digital systems, via big data search and targeted espionage, military, civilian and private.
* Uncertainty about the rules and behavioural norms that could apply to all these developments, and could provide yardsticks and sign posts that could help to rebuild cyber confidence.

There is no doubt that restoring confidence is a challenge to which all stakeholders in the digital world must respond. And it is not governments alone – if ever they practice the necessary moderation and responsible behaviour – that are called upon to look for remedies. As far as our group is concerned, we have embarked on a major new study which we are doing again jointly with the ITU and which will hopefully soon see the light as a UN publication under the title “The Quest for Cyber Confidence”.

One evident plank of our findings and recommendations will be the search for new dimensions of cooperation and partnership among the stakeholder community, national and international, in short for universal cyber governance. Next to more intensive generalized measures of cyber defense and resilience, harmonization of laws and establishing responsible rules of behaviour by States and non-state actors, cyber governance is a vital ingredient of cyber confidence.

There is perhaps no better guide to articulating such a transnational cybersecurity governance approach than the International Strategy for Cyberspace of the United States (2011). It offers an excellent strategic blueprint, „a roadmap allowing the United States Government’s departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation. It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action. Most importantly, it is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek”

You will share my view that it is particularly significant that this call for international partnership has come from the United States, and that the spirit of their strategic document reflects an emphasis on cyber defense and peaceful purposes, not, as is frequently presumed, on aggressive or belligerent attitudes.

In July of 2013, India adopted her National Cyber Security Strategy. In this excellent, very professionally written document the accent is clearly on national tasks, but the Strategy, in its Objective 14 also calls for “enhancing global cooperation by promoting shared understanding and leveraging relationships”. And in its operative parts the Strategy aims at “developing bilateral and multilateral relationships in the area of cyber security with other countries”. It further aims to “enhance national and global cooperation among security agencies, CERTs, Defence agencies and forces, Law enforcement Agencies and the judicial system”. These principles and intentions are excellent, and I think it is in our collective interest that India and her cyber stakeholder community move forward in terms of more concrete action.

In the context of international cooperation and especially the need to harmonize cybercrime laws world-wide it is as evident as it is important that laws on cybercrime and its prosecution are harmonized. Here the Budapest Convention on Cybercrime of 2001 has been the seminal event. As of now, 41 countries have signed and ratified it, and 11 ratifications are pending. It is regrettable that India is not yet among the signers. If the underlying thought of this passive stance is that the Convention is considered a European text, made for Europeans, that is certainly not true. Countries as distant and different as the United States, Japan, Australia and Ukraine are full members of the Convention. In the analysis of the administrators of the Convention, however, India “is among other States with laws/draft laws largely in line with the Budapest Convention”. India thus figures prominently among the 125 states that are in one or the other way substantively connected with the Convention. Their number may soon grow, as the Organization of American states has recently recommended accession to its members.

In this context I would like to make one important point: It is not only the material penal norms on cyber delinquency and the successful systematization of cybercrimes that are being harmonized through Budapest, and thus remove safe havens for criminals, but the Convention also, and perhaps equally importantly, internationalizes law enforcement and international information-sharing, 24/7 observation, early warning, transnational cooperation by CERTs, etc. in a *multilateral contractual framework*. The US International Strategy - I apologize for quoting it twice - , in also advocating broad accession to the Treaty, has the following to say: “The United States and our allies regularly depend upon cooperation and assistance from other countries when investigating and prosecuting cybercrime cases. This cooperation is most effective and meaningful when the countries have common cybercrime laws, which facili­tates evidence-sharing, extradition, and other types of coordination. The Budapest Convention on Cybercrime provides countries with a model for drafting and updating their current laws, and it has proven to be an effective mechanism for enhancing international cooperation in cybercrime cases”. What is true from a US viewpoint would certainly also be true from the perspective of other key countries that are, like India, leaders in Cyber Law.

Substantive penal cyber law is important, but the need for comprehensive norms for the responsible behavior in cyberspace by States, non-state actors and all other stakeholders goes much beyond. Cyberspace was initially a void, in need of a comprehensive framework of norms not only for States, but for all stakeholders. The task was to develop over time a set of norms for convivial behavior – of a culture of cyberspace and cybersecurity, including a comprehensive legal framework to manage and control the all-pervasive, infinite potential of digital technologies. Yet, there is as yet little or no ability to effectively control by law the escalation of cyber conflict and to guarantee the peaceful use of cyberspace, - and no unambiguous understanding of how the existing norms of international law would apply.

Fortunately, 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 and transparency measures or codes of conduct as normative tools. We may be witnessing a turning point in cybersecurity diplomacy.

The prevailing view is now that CBMs and codes of conduct 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.

There are currently many parallel international activities that jointly contribute to consensus-building. Recently, attention has centered on the UN Group of Experts with the concrete mandate to define “cooperative measures …. including norms, rules of principles of responsible behavior of States and confidence-building measures with regard to information space” The eminent participant from India has been Mr. Harsh K. Jain, Joint Secretary at the Ministry of External Affairs Their report, before the UN General Assembly in 2013, demonstrates considerable progress and a general understanding that international law and basic norms apply in cyberspace. A long list of concrete recommendations has been agreed in a general way. World-wide conferences, the latest one in Seoul, have maintained the momentum, and analytical contributions from academia and official institutes (like UNIDIR) are helpful. Indeed, a body of norms and of confidence-building measures is now shaping up. The UN are assembling another Government Experts Group to continue the task. The time is hopefully nearing when substantive proposals could be formulated, the right fora for multilateral negotiating processes be identified and modes of adoption and implementation of norms and measures can be developed. There is work for all of us.

..