

**3<sup>rd</sup> Facilitation Meeting for WSIS Action Line C5  
“Building confidence and security in the use of ICTs”**

**22-23 May 2008  
Geneva, Switzerland**

**Session 5: Overview of Stakeholder Activities: *Who is  
doing what in Cybersecurity?***

**Ambassador Henning Wegener, Chairman of the Permanent  
Monitoring Panel on Information Security of the World  
Federation of Scientists, Geneva/Erice**

I welcome the opportunity to inform this meeting about our work on cyber security within the World Federation of Scientists, to place it in the perspective of our joint work here, and thereby to help promote effective interaction and networking with others. I will also raise some action points from our point of view.

The World Federation of Scientists (WFS) was founded in Erice, Sicily, in 1973 by a group of eminent scientists; the founder president is Prof. Antonino Zichichi (CERN, U. of Bologna). The Federation has grown to include more than 10,000 scientists drawn from more than 110 countries, among them a great number of Nobel Prize winners. WFS promotes international collaboration in science and technology between scientists and researchers from all parts of the world, striving towards an ideal of free exchange of information, where scientific discoveries and advances are shared among the people of all nations, so that everyone may experience their benefits.

Concerned primarily with nuclear issues and the nuclear threat in the first decades of its activity, the WFS has for some time broadened the scope of its inquiry, without abandoning its nuclear focus, to what it calls “planetary emergencies”, time-critical phenomena that epitomize the fragility of modern society and endanger stable human development, - and therefore call for

urgent and coordinated international responses on an interdisciplinary basis. Some prominent area headings are energy, climate, biotechnology and new diseases, water and desertification, extreme weather events, pollution, and, lately but intensely, terrorism. Working groups designated as permanent monitoring panels deal with the identified calamities in a strictly interdisciplinary mode. In the framework of the sister organization, the International Centre for Scientific Culture (ICSC)/World Laboratory, specific pilot projects are developed and implemented to mitigate the Planetary Emergencies. An important concomitant aim is to support scientific elites in developing countries in projects aimed at the solution of their particular problems.

Since the nineties, in the course of its International Seminars, the WFS has identified the threats emanating from cyberspace as a major indicator of the fragility of modern, integrated societies and of undoubted relevance to the functioning and security of the world system, and, indeed, as an incipient planetary emergency. Early on, the WFS also recognized that the problem of information security was not only growing at an alarming pace, but that it will not be resolved by the efforts of just one state or a group of states or on a regional basis, thus calling for a unified effort of the entire international community. The Information Security Permanent Monitoring Panel (PMP) for which I speak 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.

Our group is varied in geographical distribution and disciplines represented. It is small, but interacts with the WFS community at large and aims to be more widely interconnected internationally. There is a good deal of technical expertise, but our focus is on the political and institutional aspects of cyber insecurity.

Our approach and our work projects reflect the tradition of the WFS. There is first the ingrained interdisciplinary method. Then there is our concern with national and international security: we view cyber insecurity primarily as a

possible generator of cyber conflict that transcends the individual sphere. Further, we are convinced of universal, rather than parochial cyber security strategies. Finally, we reflect our awareness of the special cyber vulnerabilities of developing countries by making proposals for building security strategies into the process of overcoming the digital divide.

Let me briefly point to some aspects of our work under these headings.

Our concern has been from the beginning that cyber crimes, with their instantaneous spread, the potential for the destruction of major societal assets and the impairment of social frameworks, are not so much – or not predominantly - a nuisance, or source of economic loss for the individual Internet user or economic entity, but a major source of peril for the nation State and the international community. Cyberwar, the use of “information weapons”, is a very real technique of war. We have again and again focussed on scenarios of a lethal combination of *simultaneous* attacks on individuals, the economy, critical infrastructures, and national defense assets. Without trivialising the economic dimension of cyber attacks and the exponential growth of organized economic cyber crime, our focus, frankly, has been cyber conflict, the evolving face of cyberwar, including the current emergence of cyberterrorism. In our papers and discussions we have attempted to capture the alarming new trends towards these forms of international cyber conflict, and have also analyzed the relationship of cyber attacks to extant international law. We have noted with interest that also NATO, beyond the secrecy of its work, has now given public expression to its concern with the need for collective cyber defense in its recent Bucharest Summit Declaration; indeed, we have been in touch with the NATO Secretariat on these matters. We have repeatedly called for work on an amplification of international law to encapsulate cyberwar or lesser transborder hostile actions by states or non-state actors. It is presently unclear how traditional international law pertains to cyber-attacks and how "information weapons" are to be dealt with in the laws of armed conflict. At the highest echelon, the cybersecurity issue requires

examination and interpretation of the United Nations Charter (which was of course not drafted with the cyber-age in mind). How do cyber-attacks and information warfare relate to the terms of the charter? A key concept needing elucidation is the Charter term "armed attack". Could the use of ICT to cause, or entail, death and destruction in another State automatically be considered such? This to us appears to be an urgent action point. The written and digital versions of my presentation contain references to some of our documents in this area.

A further guiding thought of our work has been the overriding necessity of global action, specifically legal, to ensure information security. The global nature of cyberspace requires global approaches. It is thus not by accident that our first major contribution to the WSIS process bears the title *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*. In this early document and its recommendations we make the case for a comprehensive international Law of Cyberspace – a concept now further developed in a UNITAR study by one of our members, Ambassador Ahmad Kamal - , and assign the leading role in ensuring the functioning and protection of cyberspace to the United Nations, including with a number of organizational proposals. These are now happily superseded by the organizational set-up adopted in the Tunis Agenda for the Information Society, creating a nascent International Cybersecurity Regime with a determinant role for the ITU. The UN role and the need for ever-closer international cooperation in fighting cyber insecurity are now universally accepted. We have also attempted to make intellectual inputs to the ongoing endeavour to harmonize and complete national cyber law codes.

Our third major emphasis has been on injecting more security thinking into the ICT capacity building for developing countries. Convinced that the increasing Legal Divide and Security Divide in the information age are the greatest barriers to bridging the Digital Divide, we have again and again substantiated the argument that capacity building and security building have to go hand in hand.

Our contribution to the WSIS at its Tunis phase, *Information Security in the Context of the Digital Divide*, makes concrete recommendations to this end. While our main point of argument is now well reflected in many international activities, it is to be regretted that one major forum of the global civil society specifically designed to raise the level of consciousness for the ITC needs of developing countries, the GAID, has so far excluded the security argument, and has remained insensitive – and unresponsive - to various inputs our group has tried to make to their work.

Let me now share with you some modest thoughts on what a civil society group like ours can, and perhaps *should* do. The basic idea is of course that more information, more exchange and more cooperation generate more synergies and reinforce concrete initiatives. This is the rationale behind the ITU's stakeholder activities like this most welcome meeting. For our part, the Permanent Monitoring Panel is interested in recruiting members more widely. As Associate Members they would not need to attend meetings unless they so desire, but could provide inputs and follow events. In the same logic of interaction, we would be interested in networking with other organizations in our chosen fields of endeavour.

Since the adoption of UN General Assembly resolutions on the creation of a global culture of cybersecurity (A/RES/57/239, A/RES/58/199) and the 2002 OECD "Guidelines for the Security of Information and Networks: Towards a Culture of Security" it has been universally accepted that an effective strategy against cyber insecurity requires more than mastering and implementing state-of-the-art cybersecurity technology. In rapidly changing and complex cyber environments, there is a need for creative flexibility beyond fixed rules and standards - with their periodical updates, for dynamic and innovative approaches and a novel form of interaction between security technology and people. The term "culture" is used to capture this behavioral shift, the ingrained awareness, comprehensive view of security obligations and steady vigilance by information agents required towards this end. This broad societal awareness

requires the cooperation of many. The Permanent Monitoring Panel is presently providing inputs to the work program of the ITU on an ITU Toolkit for Promoting a Culture of Cybersecurity, and I am sure collective support by other stakeholders would help the cause.

Finally, as I did last year, I would suggest that the ITU Cybersecurity Gateway, already a precious central information resource whose management merits praise, increasingly be made into the real world marketplace for information and information exchange on cybersecurity issues. This would require that as many stakeholders as possible provide topical inputs: there are synergies and higher levels of global awareness to gain.

## References

### **Toward a Universal Order of Cyberspace.**

#### **Managing Threats from Cybercrime to Cyberwar.**

Report and Recommendations. World Federation of Scientists.

Permanent Monitoring Panel on Information Security. August 2003.

Doc. WSIS-03/GENEVA/CONTR/6-E

[http://www.itu.int/dms\\_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf)

### **Information Security in the Context of the Digital Divide**

Recommendations submitted to the World Summit on the Information Society at its Tunis phase (16 to 18 November 2005)

World Federation of Scientists

Permanent Monitoring Panel on Information Security

Doc. WSIS-05/TUNIS/CONTR/01-E

<http://www.itu.int/wsis/docs2/tunis/contributions/co1.pdf>

### **The Evolving Face of Cyber Conflict and Information Warfare**

William A. Barletta

August, 2006

### **Harnessing the perils in cyberspace: who is in charge?**

Henning Wegener

UNIDIR. DISARMAMENT FORUM, 2007 – no. 3

(ITCs and International Security)

[http://www.unidir.org/bdd/fiche-article.php?ref\\_article=2646](http://www.unidir.org/bdd/fiche-article.php?ref_article=2646)

### **Homeland Security v. Homeland Defense: Gaps Galore**

Jody R. Westby

November 2007

### **The Law of Cyberspace: An Invitation to the Table of Negotiations**

Ahmad Kamal

UNITAR

November 2005

<http://www.un.int/kamal/thelawofcyberspace/>

