WSIS Action Line C5 Facilitating Meeting
Geneva, 19 May 2009

Mechanisms for Better Information Sharing – Identifying Measures for Progress – Fostering Global Partnerships

A Comment by the World Federation of Scientists

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

At last year's meeting, informing about the cybersecurity activities of the Permanent Monitoring Panel on Information Security of the World Federation of Scientists[1], I expressed the wish that the then incipient, yet already valuable ITU Cybersecurity Gateway grow into the real world market place for information and information exchange on cybersecurity issues. Since then, great strides have been made, and the Gateway is now entering a new operational phase. That is good news indeed. On the one hand, this now fully formatted information tool is bound to strengthen ITU's role as the main multilateral repository of the cybersecurity challenge, and focal point of an emerging international cybersecurity regime such as the World Federation of Scientists has been arguing for[2] since the WSIS produced its comprehensive guidelines. ITU will be even better prepared to exercise leadership and coordination in cybersecurity if it has a comprehensive data base at its disposal. On the other hand, the Gateway will fill the need of the larger stakeholder community: the synergies and the higher level of global awareness there to gain are evident and important.

Of course, the market value of the Gateway depends on two criteria. One, that all stakeholders, and that includes the private sector, academia and others, provide topical inputs and make interactive use of the Gateway; two, that the

---

[1] www.unibw.de/infosecur

[2] Henning Wegener, *Harnessing the perils in cyberspace: who is in charge?* UNIDIR. DISARMAMENT FORUM 2007 www,unidir.org/bdd/fiche.article,php?ref_article=22646

Gateway operates on a basis of conceptual clarity and comprehensiveness. It is not information that is lacking in the digital age
- rather, our curse is confusion and abundance. Thus, the challenge is structure and organization. The Gateway has now made operational a web map that aims to optimize access and relevant links and, on the whole, to allow for a balanced view of the entire problem area. Given the managerial capacities and digital prowess of the organizers, I have no doubt that the Gateway will proceed along this path and offer an ever-more coherent, semantically structured data system, - an essential step beyond the unsophisticated data access that current general search machines provide.

In this context, however, I would like to offer a caveat. As the Cybersecurity Gateway is a piece of work in progress, I do not mean to sound critical, but constructive. For an organization as mine that has been predicating much of its work on analyzing and combating cyber conflict – cyber terrorism, cyberwar, deliberate attack on critical national infrastructures - , it is difficult to understand that this topic is hardly discernable in the catalogue of organizational headings in the Gateway map. Thus, one crucial dimension of cybersecurity is definitely underemphasized. Here as in other contexts I detect a general – natural? - shyness in international organizations to face head-on a problem that obviously touches on the national sovereignties and controversies of member states, given that cyber conflict is, or would be, typically state-generated. This, however, should not prevent, and must indeed prompt serious consideration by international organizations, dedicated to the pursuit of peace as all members of the UN family, operating under the UN Charter, are. Other organizations are not so shy: UNIDIR has a sharp focus on these issues. So has the OSCE. A recent international joint seminar organized by the Council of Europe and the OAS on Terrorism and Cyber Security has tackled such issues in an unabashed manner[3]. We urge that cyber conflict be included more prominently in the contents charts of the Gateway, and that it should equally be considered as a priority topic in the ITU's Global Cybersecurity Agenda. It is also hoped that the important partnership with IMPACT and its function of

[3] www.cicte.oas.org

early-warning and emergency response to global cyber threats will include this focus.

There is no way to avoid the underlying grim realities, succumbing to the convenient temptation of trivializing them at a time when an estimated 140 nation states are developing cyber techniques in the military field and several are involved in their use for terrorist purposes. Cyber insecurity with its uncontrollable virulence and its potential for vast social harm is, apart from pervasive economic loss and societal perturbation, a major source of peril for the security of the nation-state and for international security. Cyberwar, the use of "information weapons", is a potent technique of war, and likely to be used ever more as time passes. An important focus of the papers of my group promulgated within international organizations, such as the UN, the ITU and WSIS, has been cyber conflict, the evolving face of cyberwar, and the emergence of multi-faceted cyber-terrorism[4]. We have attempted to expose these alarming trends toward new forms of conflict, and have analyzed cyber attacks in the context of extant international law, including the inherited standards and rules of war and conflict. An emerging central insight which we tried to reflect is that the plethora of digital attack techniques combined with their low cost, invisibility and universal availability enables coordinated, *simultaneous* assaults on the economy, critical infrastructures and defense systems – attacks that may not only paralyze a national state, but indeed spell disaster in multiple forms. Cyberspace favors the offensive.

We have found it necessary to highlight the special military concerns and target zones in cyber attacks. The military know the growing vulnerabilities of their operating systems and applications. They know what damage Trojans lurking in a long-duration watch-and-wait stance can do to reveal information on military planning and vulnerabilities. They know that unobtrusive attacks can neutralize or redirect weapons systems and make defenses non-functional or unreliable. They appreciate the danger of loss or manipulation of crucial coordinates – for example, the global positioning system data required for

[4] www.unibw.de/infosecur

attack accuracy. They are also aware that even the creation of protected intranet systems decoupled from public lines do not make their digital traffic per se invulnerable.

This new world of cyber conflict is not a world of established certainties and acquired wisdom. A general haziness abounds: uncharted waters. Cyberdefense is still an immature discipline. Law enforcement cooperation in the case of hostile state-sponsored network operations is a delicate undertaking and demands highest attention. In the first place, we face a definitional calamity. As cyber attack techniques – easy to practice with a few specialists and a few machines - are basically the same from bank fraud and phishing to manipulating the integrity of weapons systems, to espionage and to organizing terrorist conspiracies, a clear delineation between the various uses of ICTs is a troubling task. Despite some insightful literature, we have no clear view of what cyber weapons are. Neither, given the nature of the technology, can we distinguish clearly between offense and defense. Rather we have to deal with a sliding scale of various abuses of ICT, with clear definitions still eluding us.

Hence, the difficult challenges and uncertainties inherent in creating, or even discussing, cyber warfare doctrine and rules of engagement. Compounding this challenge is, of course, the difficulty of identifying, reliably and in a useful time frame, the origins of an attack. The attribution challenge is specifically critical in military and diplomatic matters; how can one apply international law including the laws of war, if there is no known adversary?

Another gross uncertainty is the real dimension of the threat in terms of national survival. Cyberwar operations are likely to be most successful where there are major infrastructures to attack; the more sophisticated national ICT structures, the greater the exposure. Given that simple truth, any evaluation of what it means that such a vast number of countries have cyber weapon developments under way clearly engenders uncertainty, with chilling scenarios by no means excluded. One must assume that massive DDoS attacks, disruption of

communications, the paralysis of infrastructures, ruptures in vital supply chains, are certain to cause severe havoc, or, in the worst case, national defeat. Some doubters – under the caption of "cyberwar – myth or reality?" – nevertheless minimize the effect of hostile cyber operations, at least if not accompanied by all-out military action. But such views neglect their scaling-up potential. We maintain that cyberwar is a true challenge to World Peace, and cyberterrorism, equally, a threat of global significance, with an in-built tendency for unleashing chain reactions even from modest events, thus threatening international stability.

In December of last year, the World Federation of Scientists organized a Seminar in Rome, in cooperation with the Papal Academy of Sciences, on the full range of these issues, - the texts are available on our web page[5]. Among the illustrious speakers, we were privileged to have the Secretary- General of the ITU, Dr. Hamadoun Touré. Pointedly, we placed the event under the title "The Quest for Cyber Peace", - a term not used hitherto. I would like to underline the logic of this premise and its utility for the work of the ITU. However menacing cyber conflict, the positive wording, the emphasis on the desired outcome, peace, reminds us of our goal perspective and of our moral duty to enable peace. Dwelling on the dark side of the digital age is only meaningful, if we maintain our vistas fixed on its benefits and on our joint objective to harvest them. "The Quest for Cyber Peace" has since been the caption for our on-going discussions with the ITU, and my group has proudly accepted to work with them on short notice on a book with that inspiring title. A title that stimulates our search for positive responses and thus possesses heuristic value. We will also put our own future work in the Permanent Monitoring Panel on the various manifestations of cyber conflict under this formula.

The concept of cyber peace needs of course to be fleshed out further. At first blush, it needs to be more specific than the call for a global culture of cybersecurity in response to so many UN resolutions. The emphasis must be

[5] www.unibw.de/infosecur

on the harnessing of cyber attacks with political and military – not merely economic – intent. The protected goods must include peace in the narrower, but also in a wider sense: Internet stability, security and trust, guarantee of fundamental rights and access to information in cyberspace, the unimpaired functioning of vital infrastructures. As I suggested in my earlier list of key problems in tackling cyber conflict, the emphasis must be on international cooperative action and the development of international law to accommodate cyber war offensive and defensive activities, including the aspects of cyber terrorism, thus making it operative for the cyber age.

These legal tasks, but also the impending assignments in the policy and technical field that are needed to underpin the establishment and maintenance of cyber peace, are the subject of a document entitled “Top Cyber Security Problems That Need Resolution” which the Permanent Monitoring Panel has recently elaborated and submitted to the ITU. Its primary purpose is to focus on the essential, and to provide orientation for research and collective political action, thus identifying measures for progress. It is my honor to put this list, in a slightly revised version, today also before this meeting[6]. We hope to give it wider distribution, will continue to work with interested stakeholders to refine the compilation, and will update and reissue it accordingly.

[6] Available at www.unibw.de/infosecur