The Role of Science in the Third Millenium

Plenary Meeting on Information Security: Cyber Conflicts and Cyber Stability - Finding a Path to Cyber Peace

Introduction: Science as a Prime Mover in the Construction of a Safe and Stable Order of Cyber Space

Henning Wegener

Refocusing on the role of science and applied science as the motor of progress, in an interdisciplinary setting, is nowhere more apposite than in the further expansion and development of the digital world. Information and Communication Technologies (ICT) increasingly become the new dominant paradigm of all aspects of human endeavour, providing the all-encompassing operative system of human societies.

The optimal functioning of this operative system and the realization of its development potential are thus ever more crucial.

In its work over the last few years, the PMP has concentrated on the significance of shielding information and vital systems from the impact of conflict and hostile intervention – through cybercrime, cyberterrorism, cyberwar. Their significance is undiminished indeed. Information security in this primary sense, the reliability, integrity and trustworthiness of information and networks and their effective defense, remain top global values, a public as much as a private good.

Lately our work has given emphasis to the incipient concept of *cyber peace*, a concept which the PMP perhaps more than others has helped to develop. In this work it has become increasingly clear that cyber peace not only presupposes the absence of attack and conflict. The concept is shaping up as broader, as going beyond damage wilfully inflicted.

Cyber peace requires an overall context that enables the functioning of digital systems and the generation of their benefits. As we have frequently stressed, important other ingredients include widely accepted codes of peaceful conduct, modes of cooperation, - indeed, as our PMP has stipulated early on, a “universal order of cyber space”. But risks and threats that arise from technological causes must also be assessed and harnessed. This gradual conceptual shift is clearly visible in our latest papers on Internet stability and cyber peace, as for instance in the Erice Declaration of last year. Stability and the concept of cyber peace are closely intertwined. We must be concerned not only with hostile intent and behavior, but also with the technical underpinnings of the digital world and threats emanating therefrom. Vulnerabilities stem from multiple causes.

Among the stability requirements are first the accessibility and technical prowess of digital systems, their performance characteristics and capabilities, interoperabilities and time-critical system resiliencies.
Cyber space becomes unstable not only as a consequence of deliberate attacks (often with unpredictable consequences and snow-ball effects) but also if important technical resources are unavailable, or fail through technical defects or operational errors, invalid data, or software aging. Performance, technical dependability, and integrity (as the absence of hostile intervention) are thus the triple hallmark of cyber stability, and beyond it, cyber peace.

Mastering these three major impact factors becomes more crucial and difficult as the complexity of digital systems and processes continues to grow exponentially, propelled by an accelerating rate of innovation, a revolution in connectivities, miniaturization, automation and advanced microprocessor technologies. We are witnessing a complexity explosion.

The scientific methods and technical tools for the mastery of this complexity explosion, but before all the top-of-the art conceptual scientific thinking they require, have not yet been fully developed. Essential steering functions, scientifically founded, need to be introduced and applied to key sectors of

human endeavour, including the future world economy. The scientific management challenges include the transition to new control paradigms which will necessarily include autonomous and bio-analogous control systems. These may – or will - result in the emergence of system behaviors as yet unexplored, and in all probability leading to critical impacts on cyber stability. The protection of Critical National Infrastructures and the optimization of industrial control systems (SCADA) continue to present a permanent research challenge. The scientific agenda resulting from these developments is awe-inspiring.

One example of the need for sophisticated new approaches is the energy economy where the establishment of intelligent energy management nets - smart grids - is the prerequisite for grid stability and distribution efficiency in an energy economy which has to accommodate novel energy mixes, and to optimize the relationship between supply and demand in terms of energy efficiency; billions of euros could be saved in each national economy, and climate-sensitive emissions could be minimized. The advances of electromobility, indispensable in a future energy economy, depend on a new level of sophistication in embedded systems and on network connections between vehicles and their energy environment.

The emergence of huge new smart nets to cope with the economic and ecological challenges of the future generates the demand for an enhanced scientific focus on the requirements, functions and capabilities of such smart grids, but also on information security needs. The WFS's recent paper on Top Cyber Security Problems That Need Resolution in one of its chapters provides a list of the scientific challenges that need to be confronted: e.g. to enhance resilient control systems, provide network interoperabilities, more robust data structures for identification and authentication, and new methods of meeting the security challenges of mobile and wireless systems, as well as cloud and grid computing. The new ITU Focus Group on Smart Grids will have an important role to play in this regard.

Our plenary meeting today is of limited duration. Fortunately, Secretary General Touré has already made an important contribution to our topic in the Inaugural

Session; he will speak to us again today. The other four presentations to follow – all by members of our Permanent Monitoring Panel - will no doubt also lead us further in illuminating our task to work towards cyber stability and cyber peace.

The author gratefully acknowledges the advice of Prof. Axel Lehmann on the technical developments described above.