Cyber Conflict v. Cyber Stability: Finding a Path to Cyber Peace

Introductory Remarks

Henning Wegener

Since the inception of our work on Information Security – the PMP was established in 2001 – it has become ever clearer that the increasing introduction of digital technologies into every aspect of civilized life has led to a paradigm shift and has ushered in a new era of human endeavor. At the same time, our well-nigh total dependence on ITC confers vital importance upon the stability, security and reliability of digital systems and networks, confidence in their functioning and integrity, and in the protection of privacy. These increasingly become prerequisites for the functioning of society as such. Information security thus needs to be ranked as an overarching societal challenge of global proportions – a planetary emergency. And year after year, while we work on the subject, the threats are growing, and posing greater challenges to scientists, politicians and, indeed, all stakeholders in our digital world.

Commensurate with the threat, information security has become more prominent in our work in Erice. Today, again, we are devoting a plenary session with outstanding speakers to the alarming perspectives of cyber insecurity. I am grateful to the WFS and to Professor Zichichi that we can so clearly focus on the issue. With this brief introduction, allow me to set the stage by ticking off those recent trends that have brought about yet another quality jump in the information emergency.

With 1.6 bn computers on-line, billions of micropocessors employed in embedded systems, RFID, mobile devices, ultra-miniaturization of digital circuits and the resulting ubiquity of new miniaturized computing elements leading to different and novel structures of processing configurations in digital nets, the steady progress towards an “Internet of Things” with miniature

computers inserted in cloths or the frames of eyeglasses, the development of minute computers with self-organizing potential, able to communicate autonomously with other digital devices, new human mind-machine communications (to name just some of the “next generation” trends), we are witnessing an explosive growth of digital actors and an exponential growth curve of interconnectivities, an all-pervasiveness that automatically spells a parallel increase in vulnerabilities.

The phenomena of *migration* – migration of fixed line telephone to mobile systems and to VoIP, migration of computing processes, software management and data storage from individual and business computers to huge server farms with petabyte capacity – and *convergence* – resulting in an undistinguishable mesh of mobile and fixed systems – add up to a huge integrated network structure with a universe of connectivities – and vulnerabilities - that defies quantification. It includes a myriad of important components that lie totally open to attack.

Momentous changes, thus, on the “supply side” of cyber insecurity. But even more momentous are those on the “demand” side. Past the romantic era of the individual playful hacker. We have entered the epoch of mega-cyberfraud through huge cybercrime syndicates with technical supremacy, unlimited financial resources, and an implacable thirst for fraudulent money grabbing. Attack techniques have entered a new phase of sophistication and resilience, with breathtaking speed. Any potent buyer, hostile governments and terrorists included, can unscrupulously avail himself of these potentials. The balance of attack vs. defense is tilting. We will be told about the mischief and threat potential of this new class of invisible enemies during our session.

The new key word of cyber insecurity is cyber conflict. We have crossed the threshold to an increasingly interdependent digital world in which the economy, critical infrastructures and national security can be attacked simultaneously and massively by data theft and data manipulation, DDoS, and

logic bombs. The fragility of our societies becomes more evident than ever before. Not only the stability of the Internet, the stability of society is at stake.

Cyberwar is a real threat. Trivializing it will demand a high price.

This situation calls for a new level of strategic responses, - they are the topic of today's session. Moving beyond wailing and deploring, remaining at the level of concerned analysis, we must move towards the establishment of a positive order of the digital world: to the requirements of stability, and cyberpeace. The Erice Declaration which will be proposed today is designed to commit the scientists assembled at Erice, and through them the world at large, to work on dedicated responses. Difficult tasks that need hard work, courage and imagination. And even more ambitious tasks await us, like deligitimizing like a delegitimizing the use of cyber technology for offensive military operations and strategic planning to that effect; they cannot be cannot be omitted from our action agenda. Science as an instrument for peace has always been the underlying ethics of our gatherings. Once again, Erice can make a major contribution to a more peaceful world, to creating a "global culture of cybersecurity", by showing the way to cyber stability and cyberpeace.