WORLD FEDERATION OF SCIENTISTS
PERMANENT MONITORING PANEL ON INFORMATION SECURITY

The World Federation of Scientists (WFS), founded in Erice (Sicily) in 1973, is a free association which has grown to include more than 10,000 scientists drawn from 110 countries. The Federation promotes international collaboration in science and technology between scientists and researchers. One of its principal aims is to mitigate planetary emergencies. A milestone was the holding of a series of International Seminars on Nuclear War, beginning in 1981, which have had a tremendous impact on reducing the danger of a planet-wide nuclear disaster, ultimately contributing to the end of the Cold War. Today, the WFS has focused on Terrorism, as part of its Cultural Planetary Emergency, and has held special plenary sessions and dedicated seminars at the Ettore Majorana International Centre for Scientific Culture, to address this growing threat.

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. Today, information security is an important priority. Because of the global nature of cyberspace and the more active use of information and communication technologies (ICTs), this problem is of a universal and transnational character that touches upon all facets of the existence of states, society, and individuals. The vulnerability of global and national information infrastructures gives birth to new challenges to national and international security, business activity, and human rights. The problem of information security will not be resolved by the efforts of just one state or a group of states or on a regional basis. The solution of this problem demands a unified effort of the entire international community.

In the framework of the seminars on Planetary Emergencies, the World Federation of Scientists' Information Security Permanent Monitoring Panel (PMP) 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.[1] The PMP is a multinational, multidisciplinary group of scientific, technical, legal, military, business, diplomatic, and academic experts. The Report and Recommendations of the PMP on Information Security, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar* (Report), is part of an ongoing effort that has been undertaken by the WFS to address threats in this arena. The 2003 Plenary Session of the International Seminar on Planetary Emergencies has given its endorsement and full support to the document.

This Report offers a convincing analysis of the damaging potential of cyber attacks on almost all aspects of human endeavor. Its Recommendations make the case for urgent international action in the direction of a universal order of cyberspace for which, at this juncture, only rudimentary provision has been made. They offer an urgent challenge to international decision-makers, with a special emphasis on the responsibilities of the international scientific community. The World Federation of Scientists feels that it is now of primary importance to give this Report and Recommendations wide distribution, and to put it without delay before those representatives of the international community who are in particular called upon to make their contribution to the emergence of a universal order of cyberspace.

A set of thirteen Recommendations set out in the Report were adopted by the PMP in August 2002 and endorsed by the World Federation of Scientists. In September 2002, prior to the inauguration of the 57th session of the UN General Assembly (UNGA), these Recommendations were submitted to the Secretary General of the UN, the President of the General Assembly, and the Presidents of the relevant Main Committees. In the opinion of the PMP, these Recommendations retain their validity, and the Report's Explanatory Comments are designed to provide them with new thrust and clarity. Additionally, the WFS and the Information Security PMP were represented at the World Summit on the Information Society, and its Report received the attention of UN and national leaders. The full Report is available at http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf.

[1] In the context of the work of the PMP and the Recommendations and Explanatory Comments herein, the term "information security" is intended to encompass the broader scope of cyber security, which includes the security of data, applications, operating systems, and networks.

The Recommendations and Explanatory Comments are supported by a series of papers written under the individual responsibility by the members of the PMP. The collection of these papers is available at http://www.itis-ev.de/infosecur.

The WFS has accepted the following Recommendations of the Information Security PMP:

1. Because of its universal character, the United Nations system should have the leading role in inter-governmental activities for the functioning and protection of cyberspace so that it is not abused or exploited by criminals, terrorists, and states for aggressive purposes. In particular it should: (a) respond to an essential and urgent need for a comprehensive consensus Law of Cyberspace; (b) advance the harmonization of national cybercrime laws through model prescription; and (c) establish procedures for international cooperation and mutual assistance.

2. Working to this end, the UN should give recognition to the work already accomplished by the negotiating parties to the Council of Europe Convention on Cybercrime (CoE Convention). The CoE Convention would draw greater strength if all parties who participated in its negotiation process were to sign the Convention if they have not already done so, and those who have were to accelerate the ratification and transformation processes. Immediately subsequent to the entry into force of the Convention, signatories should take steps to nominate and notify their Authority for the handling of mutual assistance, to participate in the 24/7 network, and to take other steps to promote international cooperation in the defeat of cybercrime as the CoE Convention foresees.

3. Cybercrime, cyberterrorism, and cyber warfare activities that may constitute a breach of international peace and security should be dealt with by the competent organs of the UN system under international law. We recommend that the UN and the international scientific community examine scenarios and criteria and international legal sanctions that may apply.

4. Within the UN framework, we recommend that a special forum undertake the synthesizing of work on cyberspace undertaken within the UN system.

5. In this context, we recommend the UN and other international entities examine the feasibility of establishing an international Information Technology Agency with the indicative mandate to, inter alia:

   - Facilitate technology exchanges;
   - Review and endorse emerging protocols and codes of conduct;
   - Maintain standards and protocols for ultra-high bandwidth technologies;
   - Specify the conditions on which access to such ultra-high bandwidth technologies be granted;
   - Promote the establishment of effective inter-governmental structures and public-private interaction;
   - Attempt to coordinate international standards setting bodies with the view of promoting interoperability of information security management processes and technologies;
   - Facilitate the establishment and coordination of international computer emergency response facilities, including taking into account activities of existing organizations;
   - Share cyber-tracking information derived from open sources and share technologies to enhance the security of databases and data sharing.

6. Nationally and transnationally, an educational framework for promoting the awareness of the risks looming in cyberspace should be developed for the public. Specifically, schools and educational institutions should incorporate codes of conduct for ICT activities into their curricula. Civil society, including the private sector, should be involved in this educational process.

7. Due diligence and accountability should be required of chief executive officers and public and private owners to institutionalize security management processes, assess their risks, and protect their information infrastructure assets, data, and personnel. The potential of market forces should be fully utilized to encourage private sector companies to protect their information networks, systems, and data. This process could include information security statements in filings for publicly traded companies, minimum insurance requirements for coverage of cyber incidents, and return on investment analyses.

8. In parallel, to the elaboration and harmonization of national criminal codes, there should also be an effort to work toward equivalent civil responsibility laws worldwide. Civil responsibility should also be established for neglect, violation of fiduciary duties, inadequate risk assessment, and harm caused by cyber criminal and cyber terrorist activities.

9. Among the specific and concrete actions that should be considered is the possibility that commercial off-the-shelf (COTS) hardware, firmware, and software should be open source or at least be certified.

10. Information security issues should also be addressed in forthcoming multilateral meetings. Regional organizations should also add to national and international efforts to combat attacks in cyberspace in their respective regional contexts.

11. International law enforcement organizations should assume a stronger role in the international promotion of cybercrime issues. The competences and functions of Interpol and, in the European context, Europol, should be substantially strengthened, including by examining their investigative options.

12. The international science community should more vigorously address the scientific and technological issues that intersect with the legal and policy aspects of information security, including the use of ICTs and their impact on privacy and individual rights.

13. The international scientific community, and in particular the World Federation of Scientists, should assist developing countries and donor organizations to understand better how ICTs can further development in an environment that promotes information security and bridges the Digital Divide.

The WFS is interested in collaborating with other organizations to develop a panel(s) in line with Recommendation # 12.

Contact:
Jody R. Westby, Esq.
President
The Work-IT Group
westby@mindspring.com