Document WSIS-05/TUNIS/CONTR/01-E
2 September 2005
Original: English

ICSC – INTERNATIONAL CENTRE FOR SCIENTIFIC CULTURE

WORLD LABORATORY
&

THE WORLD FEDERATION OF SCIENTISTS

ICSC – INTERNATIONAL CENTRE FOR SCIENTIFIC CULTURE
WORLD LABORATORY

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

Erice, August 2005

Preface

I take pleasure in presenting a package of Recommendations, accompanied by explanatory texts, to be submitted to the World Summit on the Information Society at its forthcoming Tunis phase. These Recommendations, under the title *Information Security in the Context of the Digital Divide,* have been elaborated by the Permanent Monitoring Panel on Information Security of the World Federation of Scientists. They seek to contribute to the objective of the Summit not only to bring the benefits of the information technology revolution to all, thus turning the Digital Divide, still sadly in evidence, into digital opportunities, but also to promote a global culture of cybersecurity. The underlying logic of the Recommendations is that nations and regions with an as yet nascent information society are specially vulnerable to cyber crime, cyber terrorism and even cyberwar, and are thus in need of special protection against cyber insecurity. Capacity-building in these fragile societies, and security-building must go hand in hand.

The Permanent Monitoring Panel on Information Security works in the framework of the International Seminars on Planetary Emergencies. Cyber insecurity, given the immense dangers to the stability and wellbeing of our societies that loom in cyberspace, belongs to this category of threats. The working method of the International Seminars, and of the World Federation of Scientists, in facing the challenge of planetary emergencies is an interdisciplinary scientific effort at an international scale. Information security especially requires such interdisplinary inputs: by information and telecommunication technologists, economists, military specialists, legal and administrative experts, as well as political scientists and politicians. The Permanent

Monitoring Panel has recently demonstrated both the need for, and the capacity of such interdisplinary work in its Report and Recommendations entitled *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar,* a document submitted to the Geneva phase of the World Summit. It makes the case for urgent international action to harness the global cyber threat.

Professor Antonino Zichichi
President, World Federation of Scientists

Introduction

Since its inception in 2001, the Permanent Monitoring Panel on Information Security of the World Federation of Scientists has been engaged in identifying the threats emanating from cyberspace as a major indicator of the fragility of modern, integrated societies and as a possible source of major instabilities and disfunctionalities in both national and international contexts, with a view to develop multidisciplinary solutions to the dangers that loom in the pervasive and ever growing use of information and communication technologies. This work is undertaken in the framework of the World Federation's International Seminars on Planetary Emergencies, a series of conferences with broad international participation, underpinned by the work of several specialized working groups.

In its Report and Recommendations of 2003, "Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar", the Panel, on the basis of an in-depth analysis of cyber threats, supported by a number of detailed studies, has assessed the immensely damaging potential of cyber attacks on almost all aspects of human endeavor, and has made the case for urgent international action toward building a universal order of cyberspace for which, at this juncture, only insufficient provision has been made. The document was submitted to the World Summit on the Information Society at its Geneva phase, where it was presented and discussed in a number of conference groups and panels (Document WSIS-03/GENEVA/CONTR/6). It has also been considered in a substantial number of other UN and international meetings and has been brought to the attention of the UN Secretary General and the executive heads of other international agencies. It has been used by the UN ICT Task Force on the basis of a cooperation agreement with the World Federation of Scientists.

The current document serves a somewhat more specific purpose and focuses less on the overriding perspectives of a universal order of cyberspace, as did the Panel's earlier Report. It is geared to the terms of reference of the World Summit on the Information Society at both its Geneva and Tunis phase. The Summit addresses the global challenge of building the information society, specifically in order to work towards overcoming the uneven distribution of the benefits of the information technology revolution between the developed and developing countries and within societies. In its Declaration of Principles, adopted at the close of the Geneva phase, the Summit has committed itself to "turning the digital divide into a digital opportunity for all". In this context, the Panel considers its primary mission, forcefully to instill the notion of information security into the Summit's proceedings, as the members of the Panel feel that the security problematique, given the predominance of the wider Digital Divide debate and other related topcs, has not yet received the attention it deserves, especially in nascent information societies that are at the center of the Summit's work; even though the Final Report of the Geneva phase of the Summit does indeed recognize that the benefits of ICTs, for their optimum realization, require that the risks caused by the threat of computer-related crimes be minimized[1].

The underlying central premise of the work of the Permanent Monitoring Panel is to help ensure that the full benefits of the information age accrue to all users of ICTs, and that they are not undercut by negative use of these technologies, be it through cyber attacks on digital archives, the flow of messages, and information infrastructures, or be it through denials of access and service. In the view of the Panel it is important to

[1] There are also several references to the importance of information security in the Declaration of Principles adopted by the WSIS Geneva phase, e.g. in paras. 19 („increase confidence and security in the use of ICTs"), 35-37. In the Plan of Action, cyber security is addresses in some detail in C5/para.12

safeguard the integrity and privacy of communications and thus the full confidence in ICTs and their security, but also to protect such essential electronic capabilities as are needed for economic growth and development. Nascent information societies – those that are, in common parlance, on the "other" side of the Digital Divide - are facing particular vulnerabilities that need to be addressed. In upgrading these infrastructures, a security element must be incorporated from the inception of the process.

The accent thus placed on the requirements of information security is particularly apposite if one considers that the threats looming in cyberspace have not ceased to grow, and are indeed reaching alarming proportions with current technological developments. The exponential growth of the number of computing devices and microprocessors (and, thereby, the steep growth of interconnectivities), the correponding increase of Internet use, the all-pervasive employment of digital techniques and assets in business life, the almost universal dependence of critical national and international infrastructures on digital controls, the growing sophistication of cyber attacks of all sorts, - all these offer new fronts for cybercrime and indicate new levels of cyber damage that can be inflicted. Add to this indicative list the development and imminent introduction of new computing techniques (invisible, ubiquitous, inexpensive), the emergence of digital identification embedded technologies, and the shift to mobile information technologies, one obtains a worrisome picture of the security challenges facing the information society in developed and developing countries alike.

Given this specific orientation towards the aims and terms of reference of the Summit, the following recommendations do not purport to form a cohesive whole, or anything resembling a comprehensive manual on cyber threats, but rather address selective

aspects of the vulnerabilities of nascent information societies, those of an as yet lower "infostate" (defined as the aggregation of info-density and info-use)[2]. Also, the recommendations vary greatly in degree of abstraction; if arranged on a continuum reaching from specificity to generality, they display an irregular pattern.

That there is a clear parallelism between the respective "infostate" of a society and its vulnerabilities to cyber threats, has been argued and credibly established in a number of international studies. There are findings that an as yet minimal telecommunications infrastructure – accompanied by a legal and law enforcement system with loopholes - may invite perpetraters of cybercrimes to use such countries as a staging ground or transit route for cyber attacks; and, generally, that emerging and still fragile IT structures may be disproportionately vulnerable until the systems in their entirety, at both the network and the user level, become more robust and security standards are more ingrained. There are also indications that viruses and "fast worms", in their geographic spread, follow the Digital Divide, and that the overproportionate adoption of mobile phones typical of nascent information societies make these vulnerable to worms specifically targeted on mobile devices.

The method followed in this document is similar to that followed in the Panel's earlier Report: there are a number of brief Recommendations, each followed by an Explanatory Note.

Beyond the Recommendations at hand, the Panel, for its part, intends to remain seized with the security aspects of the Digital Divide challenge as they emerge from the

---

[2] This useful term and its definition are taken from Sciadas, George (ed.), *Monitoring the Digital Divide . . and Beyond.* Orbicom, 2003. *(*http://www.orbicom.uquam.ca/projects/dd2002/2003_dd_pdf_en.pdf*).* The Panel is also indebted to the discussion of this concept in Gareth Sansom, *Computer-related Crime in*

discussions at the Summit and the documents resulting therefrom, and intends to structure its work program for 2005/2006 accordingly. Furthermore, the Group invites comments on its work, and encourages dialogue with interested parties[3].

Recommendations

Recommendation 1
Designing for Information Security

Professional and developers of ICT-software, -middleware and -hardware and others responsible for ICT innovations have a crucial role in providing the knowledge and means by which information protection can be enhanced. As home users and small- and medium-sized enterprises (SMEs) usually do not have the resources or professional skill sets to design ICT systems and their means of protection in face of the growing number of cyber incidents, there are double responsibilities for public and private institutions, and for countries to establish security procurement polices and standards.

It is therefore **recommended** to

- Establish means and processes of evaluating new ICT developments and products that might include establishing accreditation agencies, certification policies and procedures of information security enhancing measures.

- Continue development of national CERTS (Computer Emergency Response Teams) around the world, and their liaison with the international FIRST (Forum of Incident, Response and Security Teams) community. Their activities should include not only information sharing, analysis case studies and warning roles, but also a response capability operated by ICT security professionals. This will

---

[3] *the Context of the Digital Divide"*, a paper contributed to Workshop 6 at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18-25 April 2005. World Federation of Scientists, President, Prof. Antonino Zichichi, info@worldlab.ch; Permanent Panel on Information Security, Chairman, Ambassador Henning Wegener, henningwegener@hotmail.com. Documents of the Permanent Panel are available at http://www.itis-ev.de/infosecur.

improve end-user awareness and responsibilities with respect to safeguarding information, security and privacy. Unwittingly, these end users in cooperations, SME's, and at home can become a „launch point (pad)" for attacks on the basic communication and other infrastructure.

- Heighten awareness of end users in developing – as well as in developed - countries, as they acquire or upgrade ICT capabilities, of major risks, and of the importance of security policies and capabilities. This recommendation pinpoints the need especially for home users and SMEs to learn more about information protection and privacy, by, inter alia, participation in education and training programmes; the development of model education curricula and „drivers licenses" for computer users;

- Develop warning and reporting points' (WARPs, at www.niscc.gov.uk) which serve as a means information sharing about incidents at a local community and business level. These can be developed in association with local government, the local branches of the International Chamber of Commerce, and like-minded SMEs and other civil society groups. Unlike CERTs/FIRST they do not have an operational response role.

Recommendation 2
Cost-effective cybersecurity and privacy in nascent information societies

The integrated privacy and security of information for enterprise users of the internet in nascent information societies will depend upon their implementing effective procedural and technological tools to bring to life privacy and security plans and to monitor the effectiveness of and compliance with privacy and security procedures that meet at least minimal standards established and tested by expert developers of information system for small and medium sized enterprises.

The World Federation of Scientists **recommends** that the WSIS

- Initiate the development of quantitative risk management tools specifically tailored for enterprise managers in nascent information societies that include model information security plans scaled to the size and nature of the enterprise,

  templates for assessing their vulnerabilities and returns on investment for employing cybersecurity tools,

training modules to promote awareness in employees in secure computing practices and procedures.

self-help modules for conducting periodic cybersecurity audits.

- Endorse the use of network security tools including strong forensic capabilities at the early installation phases of networking hardware in nascent information societies

- Urge the articulation of a uniform, transnational legal guidelines for enterprise managers that can be embodied in the laws of nascent information societies.

Recommendation 3
An effective, transnational anti-spyware strategy

Executable applications and monitoring chips deployed without adequate notice, consent, *and* control of a computer owner and outside judicial control represent an increasingly malicious threat to the operability of personal computer systems and to the privacy of information on these systems. Moreover, the data gathered by spyware can easily be used to convert the host computer to be used as an unwitting accomplice computer in large-scale denial of service attacks. Indeed, the growing evidence that organized criminals are controlling networks of spybots (botnets) makes the development of uniform transnational criminal statues and attendant evidentiary standards imperative. As botnets can be used to attack commercial and governmental websites, DNS servers, email systems, and voice-over-internet (VoIP) services, their potential for disruption is especially severe for countries with nascent information infrastructures. Unfortunately with respect to criminal anti-spyware statutes, the legal framework is in the early stages of development.

The World Federation of Scientists **recommends** that the WSIS

- Strongly encourage adopting transnational industry wide definitions of spyware in both hardware and software forms to guide anti-spyware development.

- Initiate developing consistent, transnational guidelines and evidentiary standards guidelines that provide a uniform legal framework to stiffen

penalties for the use of spyware and give relevant national entities specific enforcement authority over spyware interlopers.

Recommendation 4
A Global Framework of Cyberlaw

The loopholes in, and the piece-meal nature of, current national legislation on cyberspace, especially on the side of criminal law and law enforcement, open vulnerabilities that enable exploitation by criminals and miscreants, and create increasing dangers to global populations, not least in countries with an as yet nascent information infrastructure. There is a clear and urgent need for uniform or harmonized legislation world-wide.

With this perspective, the World Federation of Scientists

- Welcomes the work which is being done under the aegis of the ICT Task Force of the United Nations to prepare draft proposals for a Law of Cyberspace. Discussions on this subject must obviously incorporate the view of all stake holders, namely, governments, the private sector, and civil society. It is the long-held view of the World Federation of Scientists that these discussions can take place only in a central multilateral forum for which the United Nations or one of its agencies offers the best and most convenient location.

- **Recommends** that the WSIS endorse the conclusions and recommendations of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice (Bangkok, 18-25 April 2005), in particular those of its Workshop on Measures to Combat Computer-related Crime and its underlying background paper, tending to promote the creation of a seamless world-wide system of criminal law on cybercrime and corresponding international cooperative law enforcement. The work results of the Eleventh United Nations Congress are fully in accordance with the World Federation's own previous Recommendations and, inter alia, highlight suitably the importance of the Council of Europe Convention on Cybercrime.

- **Recommends,** pending progress towards a uniform or harmonized legal order for cyberspace, especially as regards criminal law and law enforcement, that the WSIS examine the feasibility of, and possibly the initiation of steps towards, the negotiation of a Code of Behavior of Governments and the Private Sector in

cyberspace designed to impede hostile action against other countries and to create optimum legal and factual conditions for preventing cyber attacks.

Recommendation 5
Denial of information access through Internet filtering

Internet censorship through the use of advanced routers with an unlimited filtering capacity is increasingly employed by governments in a number of countries to block access to the Internet, or control such access, in a comprehensive manner, thus impairing internationally accepted norms of freedom of information and opinion. This censorship often goes beyond legitimate concerns of national security und other public interests and deprives the citizens in these countries of the full benefits of the information society. It is therefore **recommended** that the WSIS:

- Affirm unequivocally the principle of freedom of all to receive and impart information regardless of frontiers, as a principle to govern the Internet and as an indispensable element of an international information society;

- Discuss, within an appropriate conference framework, the extent and relevance of filtering practices, with a view to raising international public understanding and awareness of the danger to the freedom of information and the functioning of the information society emanating from them;

- Initiate an international monitoring procedure or mechanism to follow and clarify internet filtering practices, thus promoting the principles of transparency and accountability that should govern them, and permitting their evaluation against international standards;

- Examine the feasibility of setting up a complaint procedure available to all Internet stakeholders to enable the monitoring and evaluation of Internet censorship practices;

- Provide a forum for discussion of the responsibilities of the corporate providers of Internet filtering technologies in settings where negative use of their technologies in grave detriment of the freedom of information is to be anticipated.

- Confirm the importance of the wide-spread opening of Internet Cafés as a means for promoting the information society, and declare the inadmissibility of the closure or restriction of use of such means of access to the Internet.

Recommendation 6
Protecting the information society from cyberwar

No country is immune from the growing threats of cyberterrorism and cyberwar that may strike vulnerable societies – those in possession of inadequately protected ICT structures - with particularly devastating and destabilizing consequences. It is therefore **recommended** that the WSIS, in striving towards the fulfilment of its goals,

- Incorporate in its work programme an in-depth discussion of the potential adverse impact of cyberwar activities, in order to heighten the understanding and consciousness of ICT users in government and corporate entities with respect to the dangers associated with such misuse of the ICT systems on which their societies depend;

- Encourage specifically governments and the operators of critical national infrastructures to build adequate levels of protection against cyber attacks into those ICT systems that fulfill important societal, including economic, functions and enable the tranquil operation of the information society, including industrial infrastructures, public services and national defense;

- Given the potential of cyber attacks to constitute a breach of international peace and security, support the urgent initiation of work at the United Nations to study and clarify the scenarios, criteria and international legal implications and sanctions that may apply, and, in particular, to examine how traditional principles of international law relating to armed conflict are applicable to conflicts in the information age.

Explanatory Notes

Explanatory Note to Recommendation 1

Major technological advances and impending trends[4] in ICT are permanently transforming information infrastructures to embody ubiquitous, pervasive, and increasingly invisible computing and communication. These developments will profoundly influence our public and private way of living and have significant influence on individual privacy. Ubiquitous, pervasive (and invisible) ICT are enabled by advances in three major directions:

- Availability of ubiquitous information and knowledge processing capabilities (by a permanently increasing offer of Smart Systems, embedded systems, by wearable computers and ambient intelligent systems, and – last but not least – by application of transponders or RFID chips in all kinds of products, personal documents, etc. These trends along with
- High performance and high bandwidth networks offering an almost unlimited connectivity between all kinds of computing devices, and an
- Increasing offer of web and information logistic services most probably available within the coming years[5].

Without any doubt, ubiquitous and pervasive computing and communication will offer new benefits, but also new threats for the ICT user communities in a global and "networked" society – for governments, for private economies and industries, and for all individuals in their private life as well. We have to envision becoming "glassy" individuals and organizations if concrete standards for protection of information security and of privacy are not recognized, defined, implemented and legally accepted worldwide.

Most ICT research and product development focuses primarily on benefits arising from technological advances, new functionalities, and resulting ICT innovations, while less interest and efforts are given to information security and privacy risks. As noted by Lahlou et. al. "… privacy is only an abstract problem for computer designers… "[6]. A

---

4 More detailed data and projections are presented in Lehmann *Innovations in Information and Communications: Benefits and Threats,* The Science and Culture Series, Intern. Seminars on Nuclear War and Planetary Emergencies, 32nd Session August 2004, World Scientific, New Jersey 2005

5 ACM (ed.), *Security – A War Without End,* ACM queue, Architecting Tomorrow's Computing, vol. 3, nº 5 (Jan. 2005)

6 Lahou,S.: *Privacy and Trust Issues with Invisible Computers*; Communications of the ACM, March 2005, Vol. 48, No 3. See also Lahou, *European Disappearing Computer Privacy Design Guidelines V 1.0*, Ambient Agoras Report D 15.4; Disappearing Computer Initiative (Oct. 2003).

contributing factor why designers and developers of ICT products are not giving information security and privacy a high priority in their design may be that a majority of ICT users is neither aware of information security and privacy risks that they are accepting permanently when using uncritically ICT products, nor kowledgeable or trained how to prevent or minimize those risks. Especially in the context of how to overcome the "Digital Divide" through concrete actions, these two different groups of ICT stakeholders have to be distinguished.

Improving information security and privacy in such a setting offers new challenges. When talking about information security vs. privacy issues and measures, one should distinguish between:

- **perceived** information security/privacy measures (as subjective indicators for what users believe, or feel that they can trust), and

- **factual** information security / privacy measures (as more objective measures about what can be assured, or even guaranteed by application of preventive techniques like firewalls, cryptographic algorithms, authentication processes, or countermeasures against intrusion).

In general, there exists always a (significant) gap between perceived and factual information security/privacy. Perceived information security and privacy mostly depend on a user's basic ICT-knowledge, and potential risks taken when using these technologies. In contrast, the factual information and security measures depend on concrete education and training concerning ICT vulnerabilities, on the knowledge of concrete incidents and their fixes, on security practices, guidelines and techniques, and on evaluations security / privacy problems in real application scenarios.

Any discussion about the levels of awareness and knowledge of information security/privacy problems by "the" ICT user community must also address the Digital Divide. The Digital Divide exists not only between so-called developed and developing countries. A significant percentage of the population in developing countries does not have access to "state-of-the-art"-ICT – a problem that can be addressed by providing simple, robust, and cost-effective ICT devices and networks for work and self-education. In addition, a Digital Divide exists in the so-called developed countries between a) those having basic knowledge about and experience with the functions and usage of smart or mobiles devices, computers, embedded systems, or of hidden electronic sensors (e.g. RFID´s), and of fixed or mobile networks, and b) those lacking any knowledge and understanding about these technologies, devices and networks (for

example, elderly people). Making people aware of the every day risks of information security and privacy connected with the permanent usage of ICT requires concrete education and training specific to different kinds of ICT users. More and more over the next decade, almost everyone will be using ubiquitous (and invisible) information processing devices and networks, consciously or unconsciously. Increasing the level and variety of ICT usage without concomitant relevant education of all populations will diminish the benefits and increase the risks of information societies on both sides of the Digital Divide. These developments require worldwide attention and coordinated action, especially with respect tp the UN's responsibilities regarding briding the Digital Divide.

In this regard, the Panel´s recommendations address, on the one side, ICT-designers and developers, and those in charge of and responsible for ICT innovations. They have a professional obligation to take care of , and define, information privacy and security enhancing guidelines concerning the design of all kinds of ICT-components, and – systems, e.g. based on the European Privacy Design Guidelines. On the other side, these recommendations address specifically demands of different categories of user communities, e.g. by developing programs to improve ICT-Users awareness of information security problems, and by implementation of centers such as CERTs[7].

Explanatory Note to Recommendation 2

Flawlessly designed security and privacy policies and procedures afford little protection of institutional information assets if they are embodied only in management edicts, documentation, and software. In fact, "organizations that adopt policies but never implement nor enforce them may find these same policies to be a liability."[8] Corporate directors and officers must bring the security program to life through the people in an organization; security like safety is the responsibility of all personnel. In particular, all levels of line management bear an essential responsibility[9] that transcends sets of technical requirements that emanate from the chief information security officer, chief security officer, or legal counsel.

---

7 Wegener, H. *Learning Lessons from Cyber Attacks: Broadening the CERT Framework* NATO Forum on Business and Security, Istnabul (July 2004), also available at http://itis-ev.de/infosecur

8 Rasmussen, M., *Adopted But Not Implemented Security Policies May Be Your Liability,* Ideabyte, April 9, 2002

9 Westby, J., ed., *International Strategy for Cyberspace Security,* American Bar Association, August 2003 pp. 151 – 161, hereafter referred to as ISCS.

Bringing policy into action can be achieved through an approach of Integrated Privacy and Security Management[10] of information that embodies several components in a cycle of continual vigilance and improvement:

i. Assessments of risks[11] and liabilities[12] in the context of business function,
ii. Top management review of risks and formulation of policy objectives
iii. Design of policy[13], procedural and technological tools and evaluation of the associated costs,
iv. Top management review and endorsement of mitigation tools and costs,
v. Training[14] / commitment[15] at all levels within the organization,
vi. Implementation of tools including test and evaluation of tools
vii Monitoring[16] of compliance and enforcement,

---

10 This set of activities closely parallels the Integrated Safety Management (ISM) and Integrated Safety and Security Management (ISSM) presently promoted by the U. S. Department of Energy.

11 Typical risks include but are not limited to a) inappropriate use, b) denial of service attacks, c) file damage or destruction, d) physical attack, e) unauthorized control access, f) unauthorized user access, g) non-directed attacks such as viruses, worms. and other malware, f) spam and spam relaying.

12 In high-risk situations – for example, acquisitions, takeover attempts, shareholder suits, etc. – top management is required to obtain professional assistance or perform adequate analyses to mitigate the risks. See S. G. Schulman and U. S. Ottensoser, *"Duties and Liabilities of Outside Directors to Ensure That Adequate Information and Control Systems are in Place – A Study in Delaware Law and The Private Securities Litigation Reform Act of 1995,"* Professional Liability Underwriting Society, 2002 D&O Symposium, Feb. 6-7, 2002

13 The development of a security policy in consonance with institutional governance is discussed in ISCS, Ch. 5, Sec. B.

14 Employees and managers cannot be expected to carry out a security policy if they are not made aware of what is expected of them. " In an "optimized" organization, training and awareness efforts ... are fully integrated into employee career paths and sufficient budgets, resources, facilities, and instructors are provided for training and education programs. There is continuous improvement in business processes taking advantage of best external practices and maturity modeling with other organizations. Problems are resolved based on root-cause analysis and organization response is efficient and fast ... Automated tools and other education technology are used extensively and integrated into training and education programs. External trainers are used as needed." ISCS, at 186.

15 Due to the rapidly evolving nature of the information security threat, some experts recommend training and testing three times per year. Dale McNulty, *"Management's Role in Information Security - The 7 Top Mistakes,"* Nov. 4, 2002, www.surrex.com/changing_it_landscape/2002_11_04.html.

16 "Employee monitoring of ICT [Information and Communications Technology] usage is one of the easiest ways to monitor compliance with security policies and procedures, but it is an area increasingly fraught with legal liability. At the outset, there are wide inconsistencies in the global legal framework in this area. Under U.S. law (and in most third world countries),

viii. Annual reviews and audits,
ix. Adjustments to the security program.

This "enterprise program" of change management in the organization functions through a culture of acceptance of standards, policy and ethics by all employees and managers rather than through a regime of complex rules.

Unlike modern worker safety programs the most successful of which are based on the assumption that all accidents can be avoided, a prudent Integrated Privacy and Security Management System recognizes that some attacks on the information system have minimal negative impact and that some of these attacks will succeed. Consequently, for large enterprises that amass extensive data on cyber-attack incidents, a system based on a detailed return on investment (ROI) model[17] is both practical and consistent with the "due care" standard of liability. In the ROI approach the enterprise assesses the severity and frequency of each type of threat, the probability of its occurrence, the impact and costs (probable, nominal and maximum) incurred in a successful attack, the type of protection to mitigate the threat, and its enterprise-specific costs. One can then compare the costs of protection with the most probable value of cyber-damage avoided to determine the ROI, the cost effectiveness of individual protective measures. Not deploying countermeasures with a cost greater than the probable value of damage is both prudent and non-negligent.

Employees must comply with security policies and procedures, and management must take enforcement action taken in instances of violations. Both employee monitoring and audits are important compliance tools. Monitoring and screening, however, are fraught with legal considerations[18] and vastly differing legal frameworks around the

---

private sector employees are afforded virtually no expectation of privacy in the workplace698 and are not protected by the [US] Constitutional right to privacy." ISCS, at 187.

[17] A framework can help evaluate the costs and benefits of IT security solutions using a company's risk profile. Using an unconventional concept, this framework bases benefit on avoided risk rather than increased productivity. Lawrence Berkeley National Laboratory (LBNL) uses this framework to help demonstrate to management and auditors that it is significantly less expensive to accept some damage from cyberattacks than to attempt to prevent all possible damages. This pragmatic approach continues to enable LBNL's cybersecurity staff to optimize security countermeasure investments and reduce spending without sacrificing protection." Ashish Arora, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, Rahul Telang. *"Measuring the Risk-Based Value of IT Security Solutions,"* IT Professional, vol. 6, no. 6, pp. 35-42, November/December 2004. We expect that through the collected experience of large information enterprises have the resources to pool data and develop measures and approaches that can be transferred for the use of small and medium sized enterprises.

[18] "Under U.S. law (and in most developing countries), private sector employees are afforded virtually no expectation of privacy in the workplace and are not protected by a constitutional right to privacy. A few states have laws protecting privacy in the workplace; however, a

globe. The laws of the European Union afford the employee a higher expectation of privacy in the workplace than the U.S. Consequently multinational institutions and international enterprises, in particular, need to ensure that employee monitoring is legal within every jurisdiction where they conduct operations and conversely that sufficient monitoring is performed to meet liability standards.

Internal and external audits[19] that follow industry standards and best practices can validate compliance and due diligence. They can also measure the overall effectiveness of a security program. A strong, distributed audit system[20] should embody the following design principles:

1) Everyone is subject to audit.
2) Audits are cross-organizational.
3) Audit accuracy is measured by cross-validation.
4) Usage records are tamper-evident.
5) Audits are fully documented to include methods, findings, and recommendations and conclusions

Ideally, external audits are conducted through counsel, with the intention they be privileged as an attorney work product[21].

---

notice to employees that there is no expectation of privacy often removes their effect. According to a review of case law by the U.S. General Accounting Office (GAO), 'Courts have consistently held, however, that privacy rights in such communications do not extend to employees using company-owned computer systems, even in situations where employees have password-protected accounts.' Public sector employees are, however, afforded the Constitutional right to privacy. U.S. common law tort theories also provide employees with remedies for invasion of privacy. The European Union, however, affords much greater privacy to both information and employees in the workplace due to its comprehensive data protection laws, and the EU approach is starting to be followed globally. *Thus, companies should take care to ensure that their employee monitoring policy is in compliance with all jurisdictions where they have employees.*" The ABA *"International Corporate Privacy Handbook,"* J. Westby, ed., August 2003 at 146 – 147. (Hereinafter ICHP)
Management's failure to monitor traffic on its computer systems for illegal activities such as copyright infringement by employees can likewise lead to liability for the enterprise.

[19] ICHP at 149 – 157 presents a detailed discussion of the many factors that should be included in an internal audit program See also Deborah Radcliff, *"The Annual Checkup," ComputerWorld*, Sept. 9, 2002, http://www.computerworld.com/printthis/2002/0,4814,73993,00.html.

[20] The Information Systems Audit and Control Association, Inc.'s (ISACA's) has the goals to advance globally applicable standards for auditors with the skills necessary to perform information system auditing.

[21] With respect to audit reports, work product and attorney-client privilege may not provide blanket protection from disclosure. Limitations on these privileges are discussed in ICHP at 156 – 158.

Explanatory Note to Recommendation 3

While cyber security is not just a technological issue, it cannot be managed without up-to-date cognizance of technological trends and without continual improvement of technical tools to meet the evolving security challenge. As hackers and authors of malicious software develop new methods to circumvent and undermine security controls, security experts must counter with more sophisticated means of detecting intrusions in institutional networks and quarantining the compromised areas.

Gradually the message is getting out that firewalls are no protection[22] against insider threats, carelessness, and incompetence. In contrast powerful network IDS tools such as Bro[23] are vigilant against all anomalous activity whether initiated from outside the LAN or from within. Unlike a firewall, an IDS does not assume that any activity initiated inside the firewall is innocuous. For maximal protection an IDS system should be combined with software that monitors the host computer to detect anomalous activity, especially that which leads to root compromise or the installation of software without the express instruction or consent of the system administrator. The simplest form of anomaly detection software is anti-spyware software.[24]

Executable applications, deployed without adequate notice, consent, or control of a computer owner (spyware) represent an increasingly malicious threat to personal computer systems: CoolWebSearch renders browsers useless by changing Internet Explorer settings and installing malicious applications; KeenValue collects information about users and sends advertisements to their systems; Perfect Keylogger logs

---

[22] As firewalls neither stop traffic on allowed ports nor prevent the movement of what is already allowed through the system, they are useless against insider attacks and the far more prevalent mistakes and follies of inside users Relying primarily on the firewall is one of the seven top management errors that lead to computer security vulnerabilities. See *"The 7 Top Management Errors that Lead to Computer Security Vulnerabilities,"* The SANS Institute, http://www.sans.org/resources/errors.php. This is not to imply that firewalls are not valuable, only that they must be combined with other countermeasures in a layered defense.

[23] Bro, developed at the Lawrence Berkeley National Laboratory by Vern Paxson, is an example of an open source IDS which works well under very heavy loads in an open computing environment. Bro has now been adopted as the IDS software used by the US Department of Energy, sectors of the Department of Defense, and the Department of Homeland Security. ftp://ftp.ee.lbl.gov/papers/bro-CN99.ps.gz.

[24] A highly successful piece of anti-spyware is Spybot: Search and Destroy. http://www.safer-networking.org/en/index.html. Recently Microsoft has announced anti-spyware software. www.microsoft.com/athome/security/spyware/software/default.mspx. Reviews of various anti-spyware products may be found at http://www.firewallguide.com/spyware.htm

keystrokes users enter, putting users' personal information and passwords at risk; Marketscore redirects traffic from a host system to another that collects data before traffic reaches its final destination. Moreover, the data gathered by spyware can easily be used to convert the host computer to be used as a "zombie" (unwitting accomplice) computer in a networked collection of computers compromised by malware (a "botnet")[25] large-scale denial of service attacks. " Anti-virus experts have detected signs of a massive, well-coordinated Trojan attack capable of creating botnets-for-hire."[26] Surprisingly, an industry-wide definition of spyware is lacking to guide anti-spyware development.

With respect to anti-spyware statutes, the legal framework is in the early stages of development. At the Federal level in the US, five bills were introduced in the Congress in 2005; none have yet been signed into law. At the state level the legal framework is more advanced. [27] In the European Union, Directive 2002/58/EC (July 12, 2002), "Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector" targets specific technical means that provide access to information, store hidden information or trace the activities of users without their knowledge. Article 5(3) of this Directive requires Member States to ensure that electronic communications networks store information or gain access to information stored in the terminal equipment of users only if they have clear and comprehensive information in accordance with Directive 95/46/EC of October 24, 1995 "Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data."

Explanatory Note to Recommendation 4

---

25 For a detailed description of botnets see The Honeynet Project & Research Alliance, *"Know your Enemy: Tracking Botnets,"* 13 March 2005, http://www.honeynet.org/papers/bots/

26 For example see, Ryan Naraine , *"Triple-Barreled Trojan Attack Builds Botnets*," eWeek.com June 4, 2005, http://www.eweek.com/article2/0,1759,1823633,00.asp Also, Matthew Wall *"The web's wise guys,"* Matthew Wall, The Guardian ,Thursday June 3, 2004, http://www.guardian.co.uk/online/story/0,3605,1229875,00.html

27 "…State lawmakers are rushing to pass legislation. New antispyware laws have been enacted in the past three months in Arizona, Arkansas, Georgia, Iowa, Virginia and Washington. Utah, which led the state rush with its initial antispyware statute last year, recently strengthened its law to restrict pop-up ads and clarify penalties for violations. Spyware legislation is pending in 20 more states. Facing a hodgepodge of state laws and regulations, business and consumer groups are throwing their weight behind federal legislation that would stiffen penalties and give the FTC specific enforcement authority over spyware interlopers." J. Ostroff, Kiplinger Business Forecasts, Vol 6, May 27, 2005. http://www.compassweb.com/cob/kiplinger/200506/fighting_spyware.html

In its Report and Recommendations "Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar", the World Federation of Scientists has consistently argued in the direction of the essential and urgent need for a comprehensive legal order in cyberspace. Several of the Recommendations affirm that the United Nations should have the leading role in this endeavor. The Report and its Recommendations go to considerable length in establishing the universality of the problem and the need for international responses, principally through UN action. The document can serve as a reference for underpinning this Recommendation, obviating the need for lengthy additional reasoning.

Since the document referred to was submitted to the Geneva phase of the WSIS, the UN, in April of 2005, held its Eleventh Congress on Crime Prevention and Criminal Justice in Bangkok. For the second time in the series of these world congresses, a workshop on measures to combat computer-related crime was included in the work program of the Congress. Its findings and conclusions go in the direction of global legal solutions in an important sector of cyberlaw, i.e. penal law and law enforcement. The results of the Congress are of obvious significance to the WSIS, and should receive additional endorsement in this framework, as they effectively support and protect the infrastructures of the global information society, not least in the developing phase of nascent information societies. For these societies it is particularly important to affirm that countries where legal protections are inadequate will increasingly be less able to compete in a global environment and the new economy.

Both national and international regimes governing cyberspace are as yet inadequate. True enough, in most countries, especially those where the information revolution has been most marked, national legislators have acted early on to provide, e.g., sanctions and procedures for crimes in cyberspace. From the beginning, cyberspace has not been allowed to remain an area free of law[28]. Yet, no matter how well-conceived and effective many of these legislative and law enforcement initiatives on the national level, there remain considerable differences between nations of standards, legal coverage and levels of protection. Some countries have remained inactive altogether. And even more

[28] Much of the existing law (such as tort law) applicable to cyberspace results from a direct application of relevant common and criminal law. The general sufficiency of this approach was argued in an oft-cited paper by US Appelate Judge Frank Easterbrook in *The Law of the Horse,* 1996 U Chicago Legal F 20. Since the time of that paper it has become clear that cyberspace presents challenging problems with respect to jurisdictional issues, the nature of evidence, rules of custody of evidence, national norms with respect to acceptable content, and so forth. Even were it not for the existence of legal issues peculiar to cyberspace, the inherently trans-national character of the present Internet demands a uniform legal environment

is needed in terms of international equivalence of codes and international cooperation. For a computer criminal at large, there are giant legal loopholes that cannot be allowed to endure, especially in the face of the dynamics of change and growth in cyberthreats. The weakest link in the chain will be the best entry gate for roaming cybercriminals. Internationally binding and effective prescriptive instruments are needed to guide and achieve degrees of uniformity in national crime codes and procedures, and effective international cooperation in the application of measures is required. We need a universal framework of cyberlaw.

Universal, central law-making through UN treaties is, at least ideally, best suited to ensure world-wide cyberlaw. It certainly corresponds to the central role the UN must play in the ordering of cyberspace, enabling all States to participate. There are many sensible calls for the UN to be instrumental in advancing global approaches to ordering cyberspace, combating cybercrime, and establishing procedures for international cooperation.

UN treaty-making, however, is inordinately cumbersome and certainly unduly time-consuming if the treaty-making efforts were to start from scratch. An alternative method for moving towards a global framework would be to take existing treaties and broaden their affiliation. This procedure is advocated by many for the Council of Europe Convention on Cybercrime. For the existing convention with its broad coverage to be put to a more global use and thus to save precious negotiation time, it would be necessary to focus on its intrinsic merits and built-in flexibilities, and forego the luxury of stigmatizing it because of its geographical, in this case European, origin.

Another method to promote uniform international responses would be to come forward with model prescription elaborated in a UN context or by independent experts. Such texts could form a point of crystallization around which multilateral treaty-making could take place.

Alternatively, a bottom-up approach would call on States to undertake efforts at updating their cyberlaws on their own initiative, along standards “as strong” as existing legislation elsewhere. This process would work by emulation. National bodies of law would increasingly be harmonized. One important criterion for nations would certainly be that their work be compatible with a nascent global consensus.

All these methods are not mutually exclusive, but indeed mutually supportive. Neither do they weaken the central role of the UN. All might be expedited by the emergence and consolidation of an international *code of conduct,* such as recommended here, that assist in closing loopholes and increasing the approximation to a universal legal framework. The guiding principle in choosing or combining legal approaches must be

the net contribution to an effective system ensuring essential substantial equivalence of norms.

All the methodological approaches mentioned , however, face the same inherent challenges in addition to the political dilemma of striking a balance between the privacy of communication and freedom of expression in cyberspace on the one hand, and the requirements of just and speedy law enforcement on the other. All efforts are beset by the time requirements of negotiation; by often grotesquely time-consuming ratification procedures of treaties containing criminal and civil, as well as procedural requirements; by the need to transform treaty obligations into applicable national law – in fact, we are dealing with a "double transformation" - ; and by the need to ensure essential equivalence of these laws in the face of very general directive language in the international texts; further, by the time requirements for setting up functioning transnational cooperation mechanisms.

There are, however, two legal techniques that may help with the time-critical nature of the universal prescription we seek. In the first place, there is often the possibility of declaring an international undertaking provisionally applicable or of essentially following it in practice, pending the completion of the double legislative transformation process. Also, some important international agreements may be self-executing. Obligations undertaken to cooperate and lend mutual assistance in law enforcement matters, participation in alert systems, communication and information exchanges may be enacted instantly, especially where experience in transfrontier cooperation already exists.

Inserting the recommendations into the framework of the Declaration of Principles and Plan of Action adopted by the World Summit at its Geneva phase, it should be noted that the Summit documents argue forcefully for increased international cooperation in the establishment of an inclusive global information society, and in particular in building confidence and security in the use of ICTs, but are less explicit in calling for UN and international lead action in creating a comprehensive legal order in cyberspace. This relative lacuna underlines the opportunity and timeliness of the Panel's recommendations in this regard.

Explanatory Note to Recommendation 5

1.

As stated in the introduction to this document, the underlying central premise of the Panel's work is to help ensure that the full benefits of the information age accrue to all users of ICTs, and that they are not undercut by negative uses of these technologies, be it through cyber attacks on digital archives and the flow of messages and on information infrastructures, or be it through denials of access. In the view of the World Federation of Scientists it is important to safeguard the integrity and privacy of communications and thus full confidence in ICTs and their security, but also the choice to access freely the full range of information available through these technologies and principally through the Internet.

The free flow of information is a basic tenet, indeed a fundamental characteristics of free societies. Established under the auspices of the World Federation of Scientists, this Permanent Monitoring Panel feels a special obligation to support the appeal of the Erice Statement[29] to all governments to make every effort to reduce or eliminate restrictions on the free flow of information, ideas and people. This appeal is consonant with Article 19 of the United Nations' Universal Declaration of Human Rights which explicitly guarantees the freedom to "receive and impart information and ideas through any media and regardless of frontiers". The broader authority that issues from this Declaration is independent of the exact signatory status of individual countries. It establishes the basic principle of free communication through the Internet. The Declaration of Principles adopted at the Geneva phase of the World Summit solemnly confirms Article 19 in its paragraph A 4, strengthening its language, and affirming that it is central to the Information Society.

2.
Today, this principle, as internationally adopted an now again reaffirmed, is increasingly compromised not only through cyber crimes perpetrated by individuals and groups, but by the massive use of new filtering techniques by governments allowing them to restrict free access to whole categories of Internet sites, thus diminishing online freedom of expression. Modern "granular" filter technologies, developed and marketed by international technology firms, enable installation of a powerful mesh of filters that allow routers to deny access to Internet sites – or even filter out certain of their sub-pages - that contain specific key words or deal with specific issues, and beyond that, automatically track individual Internet users and identify them to the authorities for possible punishment. The use of these filter techniques and thus the introduction of massive censorship is currently taking place in a substantial number of countries, concurrently with their entry into the global information society. The broad and growing participation of the citizens of these

[29] The Erice Statement of August 1982, www. federationofscientists.com, has attracted the attention of World Leaders and has been signed by more than ten thousand scientists from all over the world

countries in Internet use is positive and of immense societal significance, but concomitant censorship deprives the users of a good part of the boost and benefits ICTs can confer upon them. These filtering practices are often supplemented by regulation that requires users to formally register their web sites lest they be shut down by an Internet police. A strong complementary measure is the closure by governments of Internet cafés. Reference is made to a series of country reports that are conscientiously drafted and kept up to date, mainly under the auspices of the private academic OpenNet Initiative[30]

Four aspects are of particular concern in this new development.

In some countries, governments use filtering techniques systematically and predominantly to block web sites with political contents. Users have no access to portals and messages that use words like "democracy", "freedom" or "human rights". The technology is thus used to infringe on political debate and freedom of opinion, and to reinforce authoritarian or repressive governments.

Secondly, the new Internet filtering techniques allow for unlimited screening and are employed by governments without any technical or institutional restraint. There are cases where whole sectors of human knowledge and endeavour and, in an era of supposed globality, information about the world at large are blocked, with attempts to transcend these arbitrary hurdles being penalized. Huge populations are left with a skewed world view.

Thirdly, although the filters can be fine-tuned, censorship is often applied broadly, so that, even beyond the purposes of the censor, a effect of undifferentiated over-blocking results, aggravating the censorship.

The fourth worrisome aspect is that those international technology companies that have developed the new techniques and produce the necessary router equipment, or the internationally active search machines that use them, are not only marketing them aggressively in the censor countries, but cooperate with, and supply technical assistance to the governments that set up Internet censorship schemes or to government-directed entities. This critique should, however, not be whole-sale, as in some cases the owners of search machines undertake to mitigate the censorship effect or offer escape routes.

3.
Censorship on Internet contents is, to be sure, not entirely avoidable, and filtering techniques can and must play important roles in safeguarding public interest. Not all

[30] http://www.opennetinitiative.net

contents are freely admissibe. Every society needs to make choices between individual rights to information and privacy, and the requirements of law enforcement and security, or basic moral values. Mesures to this effect remain in the domain of national sovereignty. It is not this principle that has undergone change, but the new complex setting in which it has to be applied .

After the 9/11 and the upsurge and menace of international terrorism operating in a trans-frontier mode, awareness of the difficult choices to be made in solving the security-versus-privacy dilemma in the Internet age and of the new security demands has risen. It has become eve more obvious that the Internet with its ease of access and global reach is not solely a source of benefits, but also has the potential for becoming a vehicle for crime and destabilization, with more than national connotations Hence the ambiguity of the new filtering techniques and the challenge of defining criteria for their use in a manner compatible with the tenets of freedom of information and access.

There is wide-spread agreement that restrictions on the use of the Internet for e.g. disseminating child pornography, instructions for creating weapons of mass destruction, incitations to racial hatred, etc. are legitimate; these also form the subject of a number of international treaties and are sanctioned by national legislation in the majority of countries.

Equally, there is no doubt that government intervention in Internet contents is legitimate to preserve security and law and order, specifically in in the context of the fight against terrorism. Governments no doubt also have the right to maintain levels of "decency" and morality within the limits of their legal system, and cultural tenets. The filtering government must, however, confront the clash of local national standards and norms with an international medium whose design resists barriers and blocks.

In general terms, especially from the standpoint of international standards of freedom of information as spelled out by Art. 19 of the UN Universal Declaration of Human Rights, these interventions should be compatible with the requirements of justifiability under national law, clearly understandable standards, proportionality, and the possibility of judicial review.

On the other extreme, however, the wholesale and undifferentiated interdiction of access to vast areas of human knowledge, the discussion of political issues and any kind of systemic criticism of policies by governments, at their will, cannot go unchecked.

Nor can the responsibility of private companies that aid and abet in enacting massive censorship and suppressing freedom of information for commercial gain be overlooked.

4.
The new forms and practices of Internet censorhip have already evoked critical responses both in the political and the academic arena. Most prominent has been the OpenNet Initiative (ONI), a collaborative partnership between three leading academic institutions[31]. ONI monitors the development and application of filtering techniques, elaborates country reports and legal analyses[32]. The Yale Center for the Study of Globalization[33] or the watchdog group Reporters Without Borders (Paris) have equally been documenting their concern and raised the problematic nature of the involvement of international technological companies. The World Press Freedom Committee, an international umbrella group of journalists' associations, has been defending press freedom on the Internet, among other activities through a major international conference endorsing guidelines for protection the freedom and independence of Internet news, and suggesting action to this effect[34].

On the political level, the US House of Representatives, on July 16, 2003, has adopted a Global Internet Freedom Act (still pending in the US Senate). The Act foresees the establishment within the US Government of an Office of Global Internet Freedom to be entasked with a comprehensive global strategy to combat state sponsored and state directed Internet interference. There are public and private organizations that encourage and finance circumvention techniques to mitigate censorship blocking of sites.

5.
These varied intitatives underline a generally perceived need for action.

In the view of the PMP, such action should ideally be untertaken internationally, as the Internet is a global instrument whose global reach and functioning is in the interest of all to preserve. The WSIS, given its broad global mandate and its UN basis, appears as the most appropriate venue for a discussion of the issue, and eventually for collective action. In any event, national action alone, such as considered within the US, would be lacking in both international effectiveness and, for some, credibility.

---

31 The initiative is a collaborative partnership between the Citizen Lab at the Munk Centre for International Studies, University of Toronto; the Berkman Center for Internet & Society at Harvard Law School, and the Advanced Network Research Group at the Cambridge Security Programme at the University of Cambridge

32 In this regard, see also the Berkman Center's study Zittrain and Edelman, *Documentation of Internet Filtering Worldwide* (last update Oct. 2003), http://cyber.law.harvard.edu/filtering

33 http://yaleglobal.yale.edu

34 http://www.wpfc.org/index

As already emerges from the nascent public discussion of the issue, the legal and political problems involved in defining the limits of internationally acceptable Internet filtering and possible sanctions are huge. Questions of national jurisdiction and sovereignty, the near impossibility of developing broadly valid borderlines between civil liberties and overriding public interests, questions of choice of law and means of enforcement, and the larger issue of Internet governance, inter alia, render an attempt at international codification unfeasible and probably futile.

Any reform of global Internet filtering must thus be looked upon in *process terms* and *strategies over time.*

The first and now necessary steps could consist in reaching a broader international understanding on the development and technical underpinning of current Internet filtering; in creating international monitoring mechanisms to further this understanding; and in promoting international public awareness.

In a second step, one might think of the introduction of an international complaint procedure, broadly accessible to all concerned and following a number of summary reporting standards.

An objective and independent country-specific evaluation of national measures giving rise to the suspicion that the freedom of information is unduly infringed upon, could be based on the findings of such a procedure. In extreme cases, recourse to the UN Human Rights Commission presently under reform might be considered.

These procedures would enhance the principles of transparency and accountability and serve to set in motion political processes and highten international public attention and pressures[35].

---

[35] A related problem – to be mentioned, but not within the purview of this set of recommendations – stems from the fact that the same advanced search techniqes that allow for systematic Internet filtering, substantially enhance the possibility of personal data collection and subsequent retention. Both through the net, and through novel RFID and smart card techniques, the permanent monitoring of a person's information uses or even physical whereabouts is now easily possible, beyond stated or legitimate purposes, and without knowledge or consent. The significance in this context is that Internet censorship can be made more effective, as attempts to access prohibited sites, or to use evasion techniques, may entail permanent policing and criminalization. Otherwise, the matter is mainly one of data protection laws and privacy (see, inter alia, the Council of Europe's 1981 *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data,* various more recent European Union Data Protection Directives, or the OECS *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.*

In a still further phase of international endeavour, the drafting of a framework of definitions and exhortative Codes of Conduct for government practices and the behaviour of industry could be undertaken.

A final issues is to what extent the development of techniques to bypass filtering should be encouraged, and their use by victims of filtering be financed. Recommendation 5 undertakes to capture most of these considerations in an operational format.

Explanatory Note to Recommendation 6

Judging by the record of the WSIS at its Geneva phase, and specifically its Final Document, the whole area of information warfare has thus far been a missing element in WSIS deliberations. Yet, it cannot be taken lighly, even in the summit context.

The threats arising from cyberterrorism and cyberwar, as those associated with cybercrime, have come to be an ever more distinct reality based on the exponential growth of the use of ICTs, the corresponding enormous growth of interconnectivities, and the ever-increasing degree to which modern, closely integrated societies depend on these technologies. If the use of cyber attacks occurs, either separately or in concert with physical attacks, or if cyber attacks are directed simultaneously against economic, infrastructural and national security assets, major societal destabilization may ensue. Countries on the "other" side of the Digital Divide are in no way immune from these threats; to the contrary, their emerging information infrastructures may be technically more vulnerable or even defenseless, and the damage to their feeble structures relatively greater. Information technologies that enable hostile use are now available to nation-states, criminals and terrorist groups, and individuals; threats may come from any of these, including from organized crime, and "virtual coalitions" of the disaffected or adventuresome. The "weapons" associated with these threats are by and large "invisible", detectable only imperfectly and at great expense, and usually after damage has already been done. Their main attributes are low cost, speed, stealth, and, unless adequately contained, a high potential for collateral damage. Yet, cyber attacks that constitute deliberate hostile action by nation-states and non-state actors alike operating transnationally may threaten international peace and security, and nevertheless elude penal sanctions under current legal frameworks.

This state of the threat presents new and complex challenges to the international community both in terms of defining what hostile actions (and adequate countermesures) are in cyberspace, and in addressing the availability and use of sanctions.

A full discussion of this problematique is offered in the Panel's 2003 Report and Recommendations[36] and its supporting papers. Specifically, Recommendation 3 of that document addresses the need for the United Nations to take action, and the international scientific community to provide the necessary intellectual underpinnings. These texts are fully relevant to the present Recommendation, and express reference is made to them[37].

The purpose of the supplementary comment offered here is to insert cyberwar activities into current tendencies of military affairs, and to evaluate their use under the established principles of the laws of armed conflict.

ICT technologies have been adopted and adapted by militaries and quasi-military movements, thus contributing to the much-cited "revolution in military affairs". Consequently, ICT are also helping to change the way warfare is planned, organized, and conducted. Intelligence, surveillance and reconnaissance; the command and control of forces and their operations; optimization of logistical movements; precision navegation and the employment of "smart" and "brilliant" weapons; and many other military applications are part of this revolution. Very significantly, it allows for the use of networks as a medium from which, through which, and in which to conduct military operations.

It is here that the potential of damage to the positive aspects of the information revolution becomes the greatest: the greater the use of ICTs, and the more tangible their link to global prosperity, the greater the vulnerabilities, and the greater the potential for collateral damage.

Cyberwarfare "weapons" may be employed against traditional targets as command and control centers, reconnaissance and surveillance satellites, transportation and logistical systems, or other kinetic forces in order to impair or destroy them. Or, they may be used to attack new targets such as the computers themselves, databases, etc., in order to deny their use, corrupt their data, or disrupt them. Cyberwarfare weapons may also be used to attack both counter-force and counter-value targets, as can more conventional weapons. Because of their very nature, and the interconnectedness of counter-force and counter-value targets in a networked world, the potential of spillover is substantial. At the same time, national or economic boundaries are negated. Cyber attacks often

[36] pp. 26-31

[37] Among the supporting papers to the Report and Recommendations, the contributions by Tsygichko, Krutskikh and Thomas are of particular relevance, all available under www.itis-ev.de/infosecur

operate in ways that defy attribution. Thus, norms related to territorial integrity and, for instance, the rights and responsibilities of neutrals are not susceptible of easy application.

Compounding the cyberwar threat and the potential response to it is the fact that only the nation-states and groups sponsored by them would appear to fall clearly within the laws of war, *jus ad bellum,* thus presenting national and international authorities with new and difficult challenges. The question is whether – and how – the norms developed for the *jus ad bellum* can also made to apply to non-state transnational actors.

As other forms of international law, the Law of Armed Conflict is composed of both customary international law and treaties, the accepted practices of the former serving to manage interstate relations even in conflictual situations. The Law of Armed Conflict applies whenever there is a state of international armed conflict and applies equally to all parties of the conflict, whether they be belligerents or neutral.

Of the general principles of the Law of Armed Conflict, the following would need examination as being particularly relevant to a networked world: the distinction between combatants and non-combatants; military necessity; proportionality; superfluous injury and indiscriminate weapons; chivalry; and neutrality.

Combatants and Non-combatants. In traditional usage, stemming from the time when combatants could see eachother on the battlefield along with their weaponry and uniforms, only a nation-state's armed forces are permitted to use force against an enemy. They must distinguish themselves from non-combattants and they may no use non-combattants or their property to shield themselves from enemy attack. This rule endures today. Applying it to cyberwarfare is problematic. One might assume that traditional nation-states take the approach of organizing and operating their cyberwar capabilities under traditional command authority and military rules of engagement. However, it is unclear whether this approach is accepted generally elsewhere. Moreover, even if cyberwarfare capabilities were organized along traditional lines, the ability to attribute the source of an attack will be murky at best. The catalytic effects caused by an unattributable third party during hostilities presents a severe challenge to the objectives of a global information society.

Military necessity. Once a state of war exists, all military assets of the belligerents (with few exceptions: military hospitals, medical vehicles, prisoners of war), and civilian infrastructures directly contributing to the war are considered hostile and subject to attack. However, civilians and their property not connected with the war effort or whose destruction provides the attacker no military advantage, may not be attacked. This principle would seem to shield purely civilian ICT structures from attack.

However, in the interconnected world in which we live, there are few purely military ICT networks. It is characteristic of the information society that everything is essentially connected to everything else. Several estimates from the United States place the US militar's reliance on the Internet at over 80%.

Nation-states with advanced technologies could be expected to to develop "surgical" information weapons in accord with this principle, but the possibility for "collateral damage" would remain high. On the other hand, lesser technologically capable belligerents seeking to employ asymmetric capabilities would be unable to develop "surgical" weapons even when trying. When faced with a conventionally superior foe, the would probably feel less constrained in using weapons of broader spread. The dilemma between perceived military necessity on the one hand, and the consequences of uneven distribution of technological prowess on the other provides another set of problems for legal judgment.

Proportionality. This principle addresses the balance between means and ends. The anticipated military advantage of an armed strike, taken in the total context of the war strategy, must be proportional to the amount of force applied, and steps must be taken to minimize collateral damage. Applying this principle to cyberwar poses special problems because of the interconnectedness of the ICT infrastructure. A power plant supporting a military installation would seem a valid military target, and a kinetic weapon might be used precisely and surgically to reduce the plan's power generation capability. Through target study, the commander could assess both the military advantage and potential collateral damage. The state of the art of cyberwarfare weapons and collateral damagde assessment methodology are much less advanced. An uncontrolled and widespread impact on a nation's power grid, its water and sewer services, and consequently on the health of the civilian population, and, beyond national boundaries, among neutrals and other non-belligerents cannot be excluded.

Superfluous injury and indiscriminate weapons. Though separate legal principles, both are discussed together here. Both categories of weapons, traditionally banned by civilized nations, are well-established. As regards cyberwarfare weapons, given the evolving nature of ICT infrastructures, the potential for superfluous injury and indiscriminate effects would appear considerable. One can imagine scenarios in which weapons are unleashed that can not be controlled, causing widespread suffering on both belligerents and non-belligerents.

Chivalry. The principle of chivalry is designed to insure that war is conducted "in accord with well-recognized formalities and courtesies". While it does not outlaw military deception, it somewhat constrains its use. Thus "perfidy" (the use of protected signs, symbols and status to deceive) is not allowed, while "ruses" (the use of trickery

that does not rely on such outer signs) are considered permissible tools. These distinctions can also be applied to the cyber age. Announcing a ceasefire over the communication media, including the Internet, when none exists, could probably be considered a perfidious act. A belligerent's ability to create the illusion of a truth or cesafire through morphing or simulation to deceive both armed combatants and the civilian populace to expose them to attack would also seem to be perfidious acts. Actions taken to corrupt data bases, create false pictures of the *status quo* on the ground, modify intelligence, etc. would seem to fall into the category of ruses.

Neutrality. A nation-state that has once declared itself neutral, assumes certain obligations not to assist either side and to prevent either side from using its territory as a base from which to attack the other. If these obligations are violated, the offended belligerent has the right to attack the "neutral". There appears to be an exception to the neutrality principle in the 1907 Hague Convention Respecting the Rights and Duties of Neutral Powers with respect to the use of communications relay systems operating from and through a neutral's territory. The language of the Convention specifies that a neutral power is not required to "forbid or restrict the use of telephone or telephone cables or of wireless telegraph apparatus" so long as such services are provided impartially to both belligerents. Ratified long before the invention of computers, fiber optics and the Internet, the Convention recognized that modern technologies had to be addressed with international law. It is unclear whether this exception would also apply to even more modern technologies with positive treaty action, although an extension by analogy would appear plausible.

Several of the afore-mentioned principles of the Law of Armed Conflict would seem to offer starting points for discussions to circumscribe the action of nation-states in conducting information warfare. Additional scholarly study will be as much required as good faith negatiations within the international community. The troubling aspect is that non-state actors and individuals engaging in cyberwar will remain outside the purview of traditional international law and its attempts at regulation. Present legal regimes are ineffective in deterring and penalizing highly relevant threat scenarios that may violate international peace and security and call for international action, specifically in a UN framework.

A key issue is that the status of information operations under Article 51 of the UN Charter, i.e. the definition of what constitutes a "force" or "armed attack" is as yet undetermined, and that the justification of the use of legitimate self-defense is, as a consequence, equally unclear. It is obvious that new, extended criteria for the definition of weapons and armed aggression should be sought. Cyber attacks on other states could then be considered acts of armed aggression unter the UN Charter, and, applying the principles of proportionality and necessity, thresholds for responsive actions in self-

defense could be defined, taking into account the direct as well as the indirect damage cyber attacks can cause. As cyber attacks are bound to increase in frequency and magnitude, bold interpretations of the UN Charter and of the laws of armed conflict will have to evolve accordingly[38].

[38] cf. Gregory D. Grove, Seymour F. Goodman, and Stephen J. Lukasik,*Cyber-attacks and International Law*, Survival, Vol. 42, No. 3, Autumn 2000, http://survival.oupjournals.org/cgi/content/abstract/42/3/89