world summit on the information society
Geneva 2003 - Tunis 2005

Document WSIS-03/GENEVA/CONTR/6-E
19 November 2003
Original: English

ICSC - INTERNATIONAL CENTRE FOR SCIENTIFIC CULTURE

Toward a Universal Order of Cyberspace:

Managing Threats from Cybercrime to Cyberwar

Report & Recommendations

World Federation of Scientists
Permanent Monitoring Panel on Information Security

August 2003

Toward a Universal Order of Cyberspace:

Managing Threats from Cybercrime to Cyberwar

Report & Recommendations

World Federation of Scientists
Permanent Monitoring Panel on Information Security

Henning Wegener, Chairman
William A. Barletta
Olivia Bosch
Dmitry Chereshkin
Ahmad Kamal
Andrey Krutskikh
Axel H.R. Lehmann
Timothy L. Thomas
Vitali Tsygichko
Jody R. Westby

August 2003

The members of the Permanent Monitoring Panel participated in their private capacity and the Recommendations and Explanatory Comments herein do not necessarily reflect the views of their organizations or governments.

Table of Contents

Abbreviations

AIPAC	American-Israel Public Affairs Committee
APEC	Asia-Pacific Economic Cooperation and Development forum
CERT/CC	Computer Emergency Response Team Coordinating Center at Carnegie Mellon University
CIDA	Canadian International Development Agency
CoE	Council of Europe
COTS	Commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency (U.S. DoD)
DCS	Distributed Control System
DdoS	Distributed Denial of Service Attack
DoD	Department of Defense (U.S.)
EBRD	European Bank of Reconstruction and Development
ELO	European Liaison Officer (Europol)
ENU	Europol National Unit
EU	European Union
FBI	Federal Bureau of Investigation (U.S.)
FDI	Foreign Direct Investment
FOIA	Freedom of Information Act (U.S.)
G8	Group of Eight
GAO	General Accounting Office (U.S.)
GBDe	Global Business Dialogue on Electronic Commerce
GIIC	Global Information Infrastructure Commission
HDL	Hardware Description Language
IADB	Inter-American Development Bank
IAEA	International Atomic Energy Agency
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
Interpol	International Criminal Police Organization
IPv4	Internet Protocol Version 4
IPv6	Intemet Protocol Version 6
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITAA	Information Technology Association of America
ITU	International Telecommunications Union
NATO	North American Treaty Organization
NCB	National Central Bureau (Interpol)
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology (U.S.)

OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
OSI	Open Source Initiative
PMP	Permanent Monitoring Panel
RCMP	Royal Canadian Mounted Police
ROM	Read-only Memory
SCADA	Supervisory Control and Data Acquisition
SMEs	Small and Medium-Sized Enterprises
TCP/IP	Transmission Control Protocol/Internet Protocol
TECS	Europol Computer System
TIA	Total Information Awareness
U.K.	United Kingdom
UN	United Nations
UNCITRAL	United Nations Committee on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNGA	United Nations General Assembly
UNITAR	United Nations Institute for Training and Research
U.S.	United States
USAID	United States Agency for International Development
WANO	World Association of Nuclear Operators
WIPO	World Intellectual Property Organization
WITSA	World Information Technology Services Alliance
WFS	World Federation of Scientists
Y2K	Year 2000

Preface

It is my pleasure to offer to the public, under the title *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar,* the Report and Recommendations of the Permanent Monitoring Panel on Information Security. This work, part of an ongoing effort, has been undertaken in the framework of the International Seminars on Planetary Emergencies, a series of conferences organized since 1981, with broad international participation, by the World Federation of Scientists at the Ettore Majorana International Centre of Scientific Culture. The 2003 Plenary Session of the International Seminar on Planetary Emergencies has given its endorsement and full support to the document.

The World Federation, founded in Erice (Sicily) in 1973, is a free association which as 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.

In the course of its International Seminars on Planetary Emergencies, the World Federation of Scientists 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. 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. In this spirit, I will transmit the document, on behalf of the World Federation of Scientists, to the United Nations, in particular to the Secretary General, the President of the General Assembly; the President of the Security Council; the President of the Economic and Social Council; the Presidents of the First, Second, and Sixth Main Committees of the General Assembly; the President of the ICT Task Force; the President of the Working Group on Informatics; as well as the President of the forthcoming World Summit on the Information Society to be held in Geneva in December 2003, and the Prime Minister of the Republic of Italy as the Head of the Government of the host country of the International Seminars and current President of the European Union. In so doing, I will strongly underline the need for all concerned to act swiftly and with determination.

Professor Antonino Zichichi
President, World Federation of Scientists

Erice, August 2003

Introduction

BACKGROUND

In the framework of the seminars on Planetary Emergencies, the 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] A set of thirteen Recommendations set out in this paper were adopted by the Panel 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 present Explanatory Comments are designed to provide them with new thrust and clarity.

The Recommendations take on special significance in the light of the forthcoming World Summit on the Information Society to take place in Geneva (Switzerland) from 10 to 12 December 2003, pursuant to UNGA Resolution A/RES/56/183. This world gathering, which is to develop a common vision and understanding of the information society and to adopt an action program for its promotion, is currently being planned by a great number of open-ended inter-governmental preparatory committees that will define its agenda. Even before the conclusion of this preparatory process, it has become clear that confidence and security in ICTs will be among the major topics to be discussed and acted upon. Consequently, the dangers of cyberwar, cyberterrorism, and cybercrime—and thus the concerns reflected in this Report and its Recommendations—are likely to be at the core of the discussions. In this perspective, it is hoped that the Recommendations, and their Explanatory Comments, will be duly considered and found to be useful by the world meeting.

OVERVIEW

The stability of modern society has been heightened by the ubiquitous nature of ICTs which pervades all aspects of human activity. Indeed, the utilization of ICTs is a recognized prerequisite to improved corporate competitiveness, government efficiency, human development, and the development of knowledge societies and economies. The Internet and capabilities of broadband networks have integrated business, government, and defense interests and empowered small and medium-sized enterprises (SMEs), enabling them to compete on a global basis. The benefits of ICTs, however, can be undercut by negative uses of these technologies in the form of cyber attacks, viruses and other malware, economic espionage, sabotage of data and systems, exploitation of networks, etc. Individuals and small groups can use ICTs against the interests of nation states. These cyber criminal acts can affect not only individual systems, but can also impact world peace and

[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.

security and undermine development efforts. The resulting damage can ignite panic, cause a loss of confidence, create uncertainty, and destroy trust in modern society.[2]

The challenges presented by cybercrime are directly proportional to the size of the problem. Since cybercrime was first identified and its dangerous potential recognized, the problem has shown rapid growth such that it challenges all ICT users—whether individuals, small businesses, multinational corporations, public sector entities, or nation states—and imposes responsibilities for cyber security upon them. The availability of tools to exploit ICT systems has markedly increased, thereby lowering the skill level needed to launch such attacks. Consequently, the number of incidents has risen dramatically.[3] The number of computer incidents reported to the Computer Emergency Response Team Coordinating Center (CERT/CC) of Carnegie Mellon Software Engineering Institute rose from six in 1988 when CERT/CC was formed to around 82,094 for 2002.[4]

Apart from the consequences for human development, there are three categories of harm flowing from cybercrime and attacks: economic consequences, disruption to critical infrastructures, and threats to national security and the capabilities of military and defense systems and first responders.

The economic damage and disruption associated with these incidents, compared to traditional crimes, is alarming. For example, the U.S. Association of Certified Fraud Examiners reported that in 2000, that the average sum of money taken in a bank holdup was US$14,000, but the average computer theft was US$2 million.[5] According to the 2002 Computer Security Institute/Federal Bureau of Investigation annual survey, the financial losses associated with U.S. computer crime rose from US$20,048,000 in 1997 to US$170,827,000 in 2002. Total losses incurred for the 1997-2001 time period was US$1,459,755,245.[6]

Cyber attacks against critical infrastructures also pose a grave problem and threaten the global nature of cyberspace. Critical infrastructures are those systems that are vital to government operations, public safety, and national and economic security. The U.S. government considers the thirteen infrastructures as critical: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, and postal and shipping.[7] The potential for cyber attacks against these infrastructures by other nation states and terrorists has alarmed governments around the globe. Because of the increasing dependency on ICTs, the vulnerability to cyber attacks against these infrastructures is steadily increasing. Since most of these infrastructures are owned and operated by the private sector, business's responsibility for cyber security with respect to these networks is

---

[2] Eduardo Gelbstein and Ahmad Kamal, *Information Insecurity: A survival guide to the uncharted territories of cyber-threats and cyber-security*, United Nations ICT Task Force and United Nations Institute of Training and Research, 2nd ed., Nov. 2002 at 1, http://www.un.int/kamal/information_insecurity (hereinafter "Gelbstein and Kamal").

[3] Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CERT Coordination Center, Special Report CMU/SEI-2002-SR-009, Nov. 2002 at 10, http://www.cert.org/archive/pdf/02sr009.pdf (hereinafter "Lipson").

[4] *See* CERT/CC Statistics 1988-2003, http://www.cert.org/stats/.

[5] Gelbstein and Kamal at 20-21, http://www.un.int/kamal/information_insecurity.

[6] Richard Power, "2002 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues & Trends*, Vol. VIII, No. 1, Spring 2002 at 10-11, http://www.gocsi.com/pdfs/fbi/FBI2002.pdf.

[7] *National Strategy for Homeland Security*, Office of Homeland Security, July 2002 at 30, http://www.caci.com/homeland_security/nat_strat.shtml.

heightened. Combating cybercrime requires significant international cooperation and preventative measures, and this is especially important in deterring acts against critical infrastructure.

Terrorists' use of ICTs to communicate and conspire and the feasibility of their launching attacks through information infrastructure is real. In fall 2001, the Mountain View, California, police department requested FBI assistance in investigating suspicious surveillance of computer systems controlling utilities and government offices in the San Francisco Bay Area. The digital snooping was being done by Middle Eastern and South Asian browsers. The FBI found "multiple casings of sites" through telecommunications switches in Saudi Arabia, Indonesia, and Pakistan that focused on emergency telephone systems, electrical generation and transmission equipment, water storage and distribution systems, nuclear power plants, and gas facilities across the U.S. Some of the electronic surveillance focused on the remote control of fire dispatch services and pipeline equipment. Subsequently, information about those devices, including details on how to program them, was found on Al Qaeda computers seized this year.

The U.S. government has expressed concern that terrorists are targeting the junctures between physical and virtual infrastructures, such as electrical substations handling hundreds of thousands of volts of power or panels controlling dam floodgates. According to a recent *Washington Post* report, one Al Qaeda laptop found in Afghanistan had frequented a French website that contained a two-volume online "Sabotage Handbook" on tools of the trade, planning a hit, switch gear and instrumentation, anti-surveillance methods, and advanced attack techniques. An Al Qaeda computer seized in January 2002 in Afghanistan contained models of a dam, complete with structural architecture and engineering software that enabled the simulation of a catastrophic failure of dam controls. Other computers linked to Al Qaeda visited Islamic chat rooms and had access to "cracking" tools to search networked computers and find and exploit security holes to gain entry or full command. Additionally, evidence obtained from browser logs indicate Al Qaeda operatives spent time on sites that offer software and programming instructions for digital switches that run power, water, and transport and communications grids. Al Qaeda prisoners have reportedly admitted to planning to use such tools. These systems are especially vulnerable because many of the distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems that control critical infrastructure are connected to the Internet but lack even rudimentary security. In addition, the technical details regarding how to penetrate these systems are widely discussed in technical fora, and experts consider the security flaws to be widely known.[8] Since September 11, the U.S. Government has identified 192 groups, organizations, or individuals linked to terrorism.[9]

Also, it is well known that civilians often take political actions against websites or business systems. In October 2000, the FBI issued an advisory warning that, due to high activity between Palestinian and Israeli sites, U.S. Government and private sector sites could become potential targets. Less than a month later, a group of hackers named Gforce Pakistan defaced more than 20 web sites and

---

[8] Jody R. Westby and William A. Barletta, "Public and Private Sector Responsibilities for Information Security," Mar. 2003 at 2-3, http://www.itis-ev.de/infosecur (citing " Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 26, 2002, http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html) (hereinafter Westby and Barletta Public-Private Responsibilities").

[9] Jody R. Westby and William A. Barletta, "Consequence Management of Acts of Disruption," Aug. 2002 at 3, http://www.itis-ev.de/infosecur (citing "G-7 to Call for Police Network," *Wall Street Journal*, Apr. 15, 2002 at A4) (hereinafter Westby and Barletta Consequence Management").

threatened to launch an Internet attack against AT&T.[10] Other direct acts of cyberterrorism include attacks by pro-Israeli and pro-Palestinian hackers on their opposing side's web sites. Pro-Palestinian hackers attacked several Israeli government sites, including those of the Knesset (Parliament), Bank of Israel, the Prime Minister's Office, and the Israeli Army.[11] The hackers also broke into several American-Israel Public Affairs Committee (AIPAC) databases, including one containing credit card numbers of members, then sent e-mails to 3,500 AIPAC members boasting of their intrusion.[12]

ICTs in the wrong hands present a new threat to world peace and national security through the offensive use of these technologies in the form of cyber warfare and cyber attacks. Nation states have developed more sophisticated capabilities to launch attacks against critical infrastructures and impair the national security of another state and its ability to defend itself. In a recent classified report, the U.S. Central Intelligence Agency reportedly expressed concern that the Chinese military may be examining methods to attack defense and civilian computer systems in the U.S. and Taiwan.[13]

One way of conceptualizing the problem is by viewing these e-attacks as information warfare. According to Russian experts:

> At present, there is neither an established classification of cyber weapons, nor clear definition of this term. The key concept for defining the subject area of information security is one of "informational weapons."[14]

The U.S. Department of Defense (DoD) defines information warfare as, "Information operations conducted during the time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" and defines information operations as "Actions taken to affect adversary information and information systems while defending one's own information and information systems."[15] Cyberterrorism has been defined by a leading U.S. expert in testimony before the U.S. Senate to be:

> [T]he convergence of terrorism and cyberspace….is generally understood to mean unlawful attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to

---

[10] *Id.* at 2 (citing "Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets," GAO Testimony of Robert F. Dacey, Director, Information Security Issues, Before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives, Nov. 9, 2001, GAO-02-231T at 3).

[11] *Id.* at 2-3 (citing Hanan Sher, "Cyberterror Should Be Int'l Crime," http://www.newsbytes.com/news/00/157986.html).

[12] *Id.* at 3 (citing John Lancaster, "Abroad at Home," Nov. 3, 2000, at A31, http://washingtonpost.com/ac2/wp-dyn/A4288-2000Nov2?language=printer).

[13] Bill Miller, "Worries of Cyberattacks on U.S. Are Aired," *The Washington Post*, Apr. 26, 2002 at A26.

[14] Vitali Tsygichko, "Cyber Weapons as a New Means of Combat," Sept. 23, 2002 at 4, http://www.itis-ev.de/infosecur (hereinafter "Tsygichko").

[15] Carter Gilmore, "The Future of Information Warfare," Dec. 28, 2001, http://rr.sans.org/infowar/future_infowar.php (citing Department of Defense Dictionary of Military and Associated Terms, Joint Pub. 1-02 at 209).

> death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples.[16]

Cyberwar is a very real technique of war, and likely to be used more and more as time passes. The U.S., for example, has developed an "e-bomb" that utilizes high-velocity electromagnetic pulses that can permanently disable electrical and communication systems.[17]

The cyberwar and cybercrime problem will continue to pose a serious threat that will require a coordinated response from industry, intelligence, military and defense, national security officials, and law enforcement. Even more disconcerting is the fact that there is not only the potential – but the likelihood – of a combination of attacks that will impair economic interests, critical infrastructures, and military and defense capabilities. According to a recently published UN report, "Cyber-crime and cyber-terrorism, and possibly cyber-war, will be an inevitable part of our future landscape."[18] Jurgen Storbeck, Director of Europol, has described the Internet as "a new sphere of life and a new scene of crime."[19]

There is an age-old and perpetual race between attack and defense, and information infrastructure will provide no exception. The legitimate interests of a state in countering cyber attacks and cybercrime, however, must be balanced against other international rights, such as those guaranteeing freedom of expression and human rights. Additionally, there is the concern that government regulation of and interference with Internet usage will impair the well-recognized ability of the Internet to foster democratization across the globe.

The problems posed by cybercrime, cyber warfare, and cyberterrorism are of a universal and transnational character that touch upon all facets of the existence of states, society, business, and individuals. Information security underlies each of these challenges. The Recommendations and the Explanatory Comments that follow serve to support the PMP's Recommendations and attempt to clarify the universality of these issues and the need for all nation states to work together to arrive at common solutions and approaches to the wide array of issues that must be addressed.

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 and contains the following contributions:

- "Consequence Management of Acts of Disruption," by Jody R. Westby and William A. Barletta
- "Cyber Weapons as a New Means of Combat," by Vitali Tsygichko
- "Guidelines for National Criminal Codes on Cybercrime," by Henning Wegener

---

[16] Dorothy E. Denning, "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000., http://www.terrorism.com/documents/denning-testimony.shtml.
[17] Anne Marie Squeo, "U.S. Studies Using 'E-Bomb' in Iraq," *The Wall Street Journal*, Feb. 20, 2003 at A3, A9.
[18] Gelbstein and Kamal at 3, http://www.un.int/kamal/information_insecurity.
[19] *Id.* at 8.

- "Heightening Public Awareness and Education on Information Security," by Axel H.R. Lehmann
- "International Information Security Negotiations," by Andrey Krutskikh
- "International Monitoring Mechanisms for Critical Information Infrastructure Protection," by Olivia Bosch
- "New Forms of Confrontation—Cyber-Terrorism and Cyber-Crime," by Ahmad Kamal
- "New Security Challenges in the Information Age," by Dmitry Chereshkin
- "Public and Private Sector Responsibilities Regarding Information Security," by Jody R. Westby and William A. Barletta
- "The Computer: Cyber Cop or Cyber Criminal?," by Timothy L. Thomas (with Karen Matthews).

The PMP is conscious of the fact that its work is of a continuous nature, and that a number of issues have not yet been adequately probed, be it within the WFS or outside. Among these are:

- The delineation between the requirements of transparency versus privacy, as well as the need to balance civil liberties and privacy protection against security and law enforcement requirements.
- The development of adequate methodologies, on the basis of comparative analysis, for risk assessment in the ICT area.
- An analysis of the opportunities and challenges in the development of wireless systems and the improvement of the security of wireless technologies.
- A review of corporate governance with a view to improved digital risk management.
- Risk analysis and audit principles.
- Identification of new research areas for further examination; e.g., application level security, fault tolerant networks, self-healing networks, autonomous response, etc.
- Strategies ad tactical warning; e.g., are these feasible? If so, what do they mean in terms of timeliness and response? Are there tools that could be developed to enable warning?
- The role of the scientific community in educating politicians, the public, and the corporate world to cyber threats/vulnerabilities and their potential impacts on "life as we know it."
- Bridging the Digital Divide (with its various sub-problems of improving access to hardware, to software, to training, and to material on relevant issues, especially those of interest to developing countries, and the identification of low-cost solutions to this end).

In its next work phase, the PMP intends to delve deeper into these issues, while also monitoring, on a systemic basis, the progress of implementation, as well as the remaining lacunae, of its current Recommendations.

Recommendations

Today, information security is an important priority for societies. 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 light of the foregoing, the Panel accepted the following Recommendations:

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.

Explanatory Comments to Recommendations

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.

A. Why Should the UN Have the Leading Role in Intergovernmental Activities on Cyberspace?

The interconnected global network of 600 million online users[20] served by 15 million hosts[21] connecting nearly 200 countries presents increasingly daunting security challenges to governments, companies, and citizens. Although the Internet has brought enormous economic and social benefits, it has also ushered in a host of new problems. Negative repercussions[22] of the Internet boom – while not outweighing the benefits – include:

Computer related fraud, forgery, and theft
Violations of intellectual property rights
Cyber-mediated physical attacks
Sabotage of data
Network attacks such as distributed denial of service attacks (DDoS)
Malicious code (viruses, worms, and Trojan horses)
Web defacements, including politically motivated hacking (hactivism)[23]
Unauthorized interceptions of communications, intrusion, and espionage
Identity theft
Spoofing of IP addresses, password cracking, and theft
Online sexual exploitation of children and child pornography
Computer harassment and cyber-stalking.

The motivation to commit cybercrime is also increasing exponentially. Ever increasing connectivity among Internet users around the globe compounds the risks because there will be more sophisticated communications infrastructure and an increased pool of bad actors and

---

[20] Westby and Barletta Consequence Management at 1, http://www.itis-ev.de/infosecur (citing Global Internet Statistics: Sources & References, Global Internet Statistics (by Language), Mar. 31, 2002, http://www.global-reach.biz/globstats/evol.html).

[21] *Id.* (citing Dave Krisula, "The History of the Internet," Aug. 2001, http://www.davesite.com/webstation/net-history.shtml).

[22] These items are described in detail in the paper by Timothy L. Thomas (with Karen Matthews), "The Computer: Cyber Cop or Cyber Criminal?" http://www.itis-ev.de/infosecur.

[23] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Internet and International Systems: Information Technology and Foreign Policy Decisionmaking Workshop, http://www.nautilus.org/info-policy/workshop/papers/denning.html.

terrorists who can use technology to conspire and to commit widespread vandalism, fraud, economic espionage, and to launch attacks on networks and information systems.[24]

The already pervasive and expanding nature of the Internet and ICTs requires a universal approach to the security of data, systems, and networks. According to a recent UN report on information security:

> The wide and pervasive integration of computers and embedded chips into modern society is what makes it vulnerable to cyber-attacks. Computers are now deeply integrated into the management and processing of our daily actions, and embedded chips are so omnipresent today that it is virtually impossible to determine even their actual numbers and locations. This became abundantly clear during the Y2K exercise, when businesses and governments spent billions to make sure computer systems would work when the year 2000 began.[25]

The profound integration of computers and information technology is obviously the strength of modern life, but it is also its vulnerability. The greater the interconnectedness, reliability, and complexity, the greater the vulnerability and the ease for exploitation. Information and communications systems are not only a potential target of criminals, terrorists, and military planners; they are also portals of physical vulnerability for the vast number of physical assets with controls linked to the Internet or managed by information technology systems. These direct and indirect vulnerabilities are amplified by the relatively small number of nodal exchange points (roughly 100 or so) on the Internet network, the existence and location of which is public knowledge.[26]

Because the ubiquitous nature of the Internet and the built-in vulnerabilities of the global network require a global perspective, the UN is ideally suited to accept a role within its capabilities to lead inter-governmental activities regarding the security of cyberspace. Similarly, only a global consensus can address the updating of the laws of war to include the parameters of wars in cyberspace.[27] No multinational organization other than the UN has the membership and capability to address these issues in a meaningful way that will have global impact. Beyond security concerns, the utilization of ICTs in investigatory, tracking, and recording practices and control over communications and Internet usage poses a serious threat to international rights guaranteed under the international law of the UN, such as human rights, freedom of expression and other civil liberties. According to a senior UN official:

> As the only truly universal international organisation that we have today, the United Nations can provide the broadest and most neutral and legitimate platform for bringing together governments and other key stakeholders to undertake this effort. Only this institution can provide the forum for discussion and debate on the complexities of the subject, and coalesce the

---

[24] Westby and Barletta Consequence Management at 1, http://www.itis-ev.de/infosecur.
[25] Ahmad Kamal, "New Forms of Confrontation: Cyber-Terrorism and Cyber-Crime," Aug. 2002 at 2, http://www.itis-ev.de/infosecur
[26] *Id.*
[27] The international law aspects of this statement will also be considered in the context of Recommendation 3 and considered in depth in papers by Messrs. Krutskikh and Tsygichko, http://www.itis-ev.de/infosecur.

> expertise that exists around the world for a proper drafting of relevant legislation that can fill the existing and growing void in cyber-law.[28]

B. Why a Law of Cyberspace?

At the outset, one must acknowledge that the call for a body of law regulating cyberspace is not uniformly accepted in the legal community. The usual arguments are that (1) there is no consensus concerning the many possible designs or architectures that may affect the functionality we now associate with cyberspace; (2) very few bodies of law are defined by their characteristic technologies; and (3) the best legal doctrine re-examines, expands, or applies existing doctrines to a new arena. Whatever the validity of such comments concerning activities within single nation states, the capability of the Internet to cut across many national jurisdictions at lightning speed argues that we look anew.[29] It recommends that nations seek a comprehensive re-examination of the many relevant, sometimes conflicting legal doctrines, practices, and procedures to produce a comprehensive, universal, and uniform legal framework for handling the issues colloquially called cyber law.

The Privacy & Computer Crime Committee, Section of Science & Technology Law of the American Bar Association, has recognized the need for international action to create a uniform body of law:

> A major component of information and infrastructure security is a nation's ability to deter, detect, investigate, and prosecute cyber criminal activities. Industrialized nations and multinational organizations have taken significant steps toward combating cybercrime. The glaring gaps in work to-date are (1) inadequate international coordination and (2) woefully deficient legal frameworks and organizational capacity in developing countries necessary to combat cybercrime.[30]

An initial framework that could serve as an excellent starting point for the development of a Model Law on Cybercrime has been developed in the Council of Europe. The CoE Convention on Cybercrime of 2001 (CoE Convention) has been signed by 36 countries.[31] Although civil libertarians and privacy advocates continue to express concern that the CoE Convention undermines individual privacy and is inconsistent with provisions in U.S. law, it has been endorsed by the Group of Eight (G8) as a model to be followed by other countries.[32] Other important work in this area has been done by the G8, the Organization for Economic Cooperation and

---

[28] Gelbstein and Kamal at 123, http://www.un.int/kamal/information_insecurity.

[29] *Id.*

[30] Jody R. Westby, ed., *International Guide to Combating Cybercrime*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, 2003 at 11, http://www.abanet.org/abapubs/books/cybercrime/ (hereinafter "Westby Cybercrime").

[31] Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (hereinafter CoE Convention); Press Release, "Budapest, November 2001: opening for signature of the first international treaty to combat cybercrime," Council of Europe, Nov. 14, 2001, http://press.coe.int/cp/2001/840a(2001).htm. The criminal law aspects of information security are further developed in Recommendation 2 and the PMP paper by Henning Wegener, "Guidelines for national criminal codes and their application throughout the international community," Jan. 2003 at 7, http://www.itis-ev.de/infosecur (hereinafter "Wegener Guidelines").

[32] *G8 Recommendations on Transnational Crime*, Section D: High-Tech and Computer-Related Crimes, item 2, http://canada.justice.gc.ca/en/news/g8/doc1.html.

Development (OECD), the Asia-Pacific Economic Cooperation (APEC), the European Union (EU), and the Organization of American States (OAS).

Furthermore, with the public revelation of President Bush's National Security Presidential Directive 16 ordering the U.S. government to develop cyber warfare guidelines and rules under which the U.S. could penetrate and/or disrupt foreign computer systems,[33] cyber warfare has come out of the closet. As with other forms of warfare, there should be internationally accepted limitations on the form of conflict. Certainly, a meaningful codification of such activities should take place under the aegis of the international body with the widest membership, the United Nations.

The PMP concludes that, on a global basis, current national and international legal frameworks are insufficient and inconsistent across national jurisdictions to address the scope and complexity of the subject of cybercrime, cyberterrorism and cyber warfare. While efforts to combat cybercrime and cyberterrorism have been valiant and even successful in many areas, more is possible. We recommend a determined effort be made to draw upon the work performed to date in order to draft and adopt a comprehensive Model Law on Cybercrime and agreement on related procedural, administrative and cooperative considerations. The UN has already performed excellent work in the development of model laws for electronic transactions and electronic signatures[34] and its institutional roots are based on established international rules for conflict. Such a Model Law would have to address numerous issues, ranging from technical and definitional (e.g., what is cyberspace) to substantive (e.g., legal provisions, jurisdictional issues, and standards of evidence) to procedural and administrative (e.g., international cooperation mechanisms). It would also have to balance competing interests of sovereignty, national security, civil liberties, human rights, and freedom of expression. The UN should give separate consideration to determining the rules under which nation states may engage in cyber warfare and respond to cyberterrorism. The World Summit on the Information Society may also be a forum for discussion on this subject.

C. How Comprehensive a Consensus is Needed?

Some argue that the CoE Convention on Cybercrime is adequate consensus for an international legal framework to be developed. A legitimate counterpoint, however, is that more countries would have to sign and ratify the Convention and abide by its terms in order for it to effectively deter cybercrime, significantly advance international cooperation on these issues, or lead to a harmonized global framework. Out of about 200 countries, only 36 have signed the CoE Convention. Many of the countries who have not signed the CoE Convention either do not have any cybercrime laws, or have such inadequate ones, that criminals can essentially act with impunity. Since communications utilizing packet switched technologies often travel through many countries before reaching their destination (even on local-to-local communications), the CoE Convention does not provide a comprehensive enough consensus in this area.

---

[33] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *The Washington Post*, Feb. 7, 2003 at A01, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38110-2003Feb6&notFound=true

[34] United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures (2001) and Model Law on Electronic Commerce With Guide to Enactment (1996), http://www.uncitral.org/en-index.htm.

However, despite some shortcomings, controversial points, and lacunae, the CoE Convention "no doubt constitutes a major drafting achievement by a representative cross section of the international community, and there is no private or public initiative in sight that could match it in legal status, completeness, quality and endorsement received."[35] This Convention deserves to be considered as a starting point for working toward a broader, universal agreement and Model Law.

D. What are Some Areas of Conflict/Inconsistency?

Multiple cases have arisen where Internet activities considered to be legitimate in one country violate the laws in another.[36] Additionally, one country may not have the procedural laws to enable it to perform the requested assistance or law enforcement may not have the expertise to assist in the search and seizure of electronic evidence.[37] Examples of areas of conflict include jurisdictional issues, extradition disputes, extra-territorial seizures, violations of content laws, and inconsistent hacking laws. These inconsistencies alone underscore the important role the UN could play in acting as coordinator on these issues.

Gelbstein and Kamal note that:

> Civil liberties groups have also expressed concern that the [CoE] convention undermines individual rights to privacy and extends the surveillance powers of the signatory governments. Critics in the United States indicate that the provisions of the convention are incompatible with current U.S. law.[38]

For example, by defining the sending of unsolicited e-mails as a criminal activity, the Convention is claimed "to criminalize behavior which until now has been seen as lawful civil disobedience."[39]

E. How Might Harmonization of Cybercrime Laws Proceed Through Model Prescription?

The UN Model Laws on Electronic Commerce and Electronic Signatures are considered to be the the global "standard" for legislation in these areas. They have been looked to and followed by industrialized and developing countries around the globe. UN action that would provide a global model law and an accompanying explanatory memoranda that nation states could use as a guide, along with an international agreement on procedural, administrative, and cooperative aspects, would make the global harmonization of cybercrime laws an achievable goal.

F. What are Examples of Procedures for International Cooperation and Mutual Assistance?

Certainly, one of the oldest and best known institutions for international cooperation and mutual assistance is Interpol. Founded in 1923, it has 178 member countries and maintains close working

---

[35] Wegener Guidelines at 7, http://www.itis-ev.de/infosecur.

[36] Lisa M. Bowman, "Enforcing Laws in a borderless Web," CNET News.com, http://news.com.com/2100-1023-927316.html?tag=fg_lede; Westby Cybercrime at 54-59, http://www.abanet.org/abapubs/books/cybercrime/. *See also* Peter Swire, "Of Elephants, Mice, and Privacy: The International Choice of Law and the Internet," 32 Int'l Law 991, 1016 (1998).

[37] Westby Cybercrime at 51-52, http://www.abanet.org/abapubs/books/cybercrime/.

[38] Gelbstein and Kamal at 118, http://www.un.int/kamal/information_insecurity.

[39] P. Meller, "EU pact would criminalize protesters who use the Net," *The New York Times*, Feb. 5, 2003, http://www.iht.com/articles/88499.htm.

relationships with numerous intergovernmental bodies. The G8, Europol, OECD, UN, APEC, and OAS have all established mechanisms or launched initiatives to promote international cooperation and mutual assistance in the cyberspace arena.[40]

One of the best known practical examples of global-scale coordinated international cooperation and mutual assistance was seen in efforts to deal with the Y2K problem.

> The Year 2000 (Y2K) experience gave rise to new ways in which governments and critical infrastructure sectors world-wide shared information to monitor incidents as they arose…..The international governmental and industry organisations notable for establishing mechanisms for global monitoring of Y2K incidents affecting critical infrastructure sectors included the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA), and the International Atomic Energy Agency (IAEA) and the World Association of Nuclear Operators (WANO).[41]

At the technical levels, there are numerous opportunities for information sharing[42] both in the public and private sectors.

> Information sharing can be facilitated by public sector initiatives that (a) establish centers for sharing information on an anonymous basis or serve as an intermediary where the direct sharing of information among industry is difficult, (b) create a central alert point for technical information and assistance regarding security risks and fixes, and (c) organize a public/private group comprised of all stakeholders (industry, government, academia, NGOs) to begin a dialogue on ICT security risks and develop ways to work together.[43]

In 1997, information sharing and analysis centers (ISACs) were established in the U.S. to facilitate information exchange among critical infrastructure sectors. ISAC members usually "share information in a way that preserves their anonymity while providing an overview of cyber incidents within their sector not otherwise obtained individually."[44] Indeed, the Commission of the European Communities notes that "urgent measures are needed to produce a statistical tool for use by all Member States so that computer related crime within the European Union can be measured both quantitatively and qualitatively."[45] This is important; however, there also needs to be a common methodological way to look at cybercrime, lest the quantity and quality results be slanted.

---

[40] Westby Cybercrime at 95-104, http://www.abanet.org/abapubs/books/cybercrime/.
[41] "International Monitoring Mechanisms for Critical Information Infrastructure Protection", Olivia Bosch, http://www.itis-ev.de/infosecur (hereinafter "Bosch Monitoring").
[42] Westby Cybercrime at 23, http://www.abanet.org/abapubs/books/cybercrime/.
[43] Wegener Guidelines at 7, http://www.itis-ev.de/infosecur.
[44] Bosch Monitoring at 7, http://www.itis-ev.de/infosecur.
[45] *Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Brussels, Apr. 19, 2002, COM(2002) 173 final, adopted by EU Ministers of Justice Mar. 4, 2003, http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf.

Information sharing efforts, however, are hindered by national laws that deter the private sector from sharing security incident information with public sector entities. Laws such as the U.S. Freedom of Information Act and other similar national "access to information laws" cause concern within the private sector that shared confidential or proprietary information may be disclosed. Antitrust laws also deter collaborative information sharing activities. Additional concerns are raised by the sharing of security incident information with foreign governments. U.S. Sentencing Guidelines create an additional risk. Corporations worry that by sharing security breach information and seeking the assistance of law enforcement, an investigation could reveal wrongdoing by corporate insiders which could "snap back" on the company and expose it to harsh penalties under the Guidelines. Thus, there is a need to develop a consistent international framework that encourages public-private information sharing by mitigating the risks that flow from these existing laws.

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.

Cybercrime defies national boundaries. Any effective strategy to prevent and combat the new types of cyber offenses and the new modalities of committing traditional offenses through technologies of cyberspace must, therefore, lead to transnational responses in criminal law and law enforcement. There must be no national loopholes; the present situation in which there are considerable differences of legal coverage, standards, and levels of protection is highly unsatisfactory. The case for a binding, universal international code of broad scope is compelling.[46]

At the same time, shared prescriptions of this nature will be unsuitable for containing and penalizing all cyber attacks. Attacks by nation states and international terrorist groups on critical societal and economic infrastructures and the defense establishment of other countries, giving rise to highly relevant threat scenarios, require different international responses, as discussed under Recommendation 3.

A number of private fora and international organizations have attempted to address the substantive, procedural, and jurisdictional challenges posed by the transnational nature of cybercrime. The most extensive is the Council of Europe's Convention on Cybercrime (CoE Convention), which was opened for signature on Nov. 23, 2001 and has, up to now, been signed by 36 countries, of which four signatories (U.S., Canada, Japan, and South Africa) are "partner" countries but are not CoE members. The Convention covers substantive penal law as well as criminal procedural law and international cooperation in law enforcement, underlining the essential

[46] Wegener Guidelines at 1-3, http://www.itis-ev.de/infosecur; Westby Cybercrime at 1-2, http://www.abanet.org/abapubs/books/cybercrime/.

linkage between the three; indeed, the time-critical nature of tracking cybercrime, securing electronic evidence, and facilitating pursuit requires such linkage.

All attempts at creating a consistent and universal penal framework for dealing with the cyber challenge have to face a number of inherent problems: (1) striking a balance between the privacy of communications in cyberspace and the freedom of expression and access to information on the one hand, and the requirements of national security and speedy law enforcement on the other; (2) the retarding influence that will be exercised by the need to ratify a treaty containing civil and criminal provisions and administrative and procedural requirements; (3) the need to transform treaty obligations into applicable law; (4) the need to ensure essential equivalence of these laws in the face of very general directive language in the international texts; (5) the time requirements for setting up functioning transnational cooperation mechanisms; or (6) the complex problem of including content-related cyber offenses. These are discussed in the accompanying papers.[47]

These difficulties notwithstanding, the CoE Convention offers great promise for moving towards a universal penal system in this field. Given the present composition of affiliated member states, it avoids the pitfall of offering a purely European focus and lends itself to a broader international audience. The ultimate objective would be to incorporate it, textually its provisions into a future Model Law on Cyberspace which is the central issue around which these Recommendations revolve.

In order to enhance the credibility and effectiveness of the CoE Convention, Recommendation 2 appeals, as a first and important step, to the parties that participated in the negotiation process to ratify and implement the Convention and to establish the necessary cooperation mechanisms for the broad geographical area which they represent.

Further steps to extend the number of signatory nation states to the CoE Convention would be welcome. Indeed, it would be highly desirable that a campaign to promote universal adherence get underway, at short notice, at the level of the United Nations, in the preparatory phase for the creation of a universal regulation of cyberspace. It would be important that response times for such an international appeal be kept as short as feasible, and that each signatory, in launching the process for transforming treaty obligations into national law, be mindful of the time-critical nature of defeating cybercrime and keeping pace with technology. If the CoE Convention can manage to create a critical momentum for the establishment of a universal legal framework and administrative organization regarding cyberspace, this momentum must not be lost.

In assessing the importance of the CoE Convention, governments should also be aware of an important complementary effort by the European Union. The EU Ministers of Justice adopted the Proposal for a Council Framework Decision on attacks against information systems on March 4, 2003. Consequently, they will now begin harmonizing their own national laws with this Decision.[48] The Council Framework Decision contains definitions, model articles for the criminalization of major cyber attacks, and rules for cooperation among EU countries, some of which flesh out in more detail provisions from the CoE text, some more concise, but overall, in

---

[47] Wegener at 4, 14, http://www.itis-ev.de/infosecur.

[48] *Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Brussels, Apr. 19, 2002, COM(2002) 173 final, adopted by EU Ministers of Justice Mar. 4, 2003, http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf.

the Framework's own professed intention, compatible with the CoE Convention. The particular level of legal and administrative cooperation that already exists among the Member States of the EU as a common legal and judicial space, but is lacking elsewhere, means that the Framework is not suitable as a model code to the same extent as the CoE Convention. The latter preserves its quality as the overriding and most complete legal instrument particularly suited for endorsement by the present Recommendation.

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.

Cyber activities that constitute deliberate hostile actions by nation states or non-state actors operating transnationally may threaten international peace and security, yet elude penal sanctions under current legal frameworks or a future Model Law on Cyberspace. One consideration is that, under certain circumstances, the international doctrine of sovereign immunity protects nation states against legal actions. This protection could conceivably extend to offensive cyber actions taken by nation states. Other concerns relate to (1) the lack of international cooperation on a global scale, and (2) technical considerations regarding the inability to effectively track and trace Internet communications.

The response to any scenario -- whether a cyber criminal activity, an act of cyberterrorism, or an intended act of cyber warfare by a nation state – requires the ability to effectively track and trace cyber attacks. A recent report from CERT/CC at Carnegie Mellon University notes:

> The capability of a nation (or a cooperating group of nations) to track and trace the source of any attacks on its infrastructures or its citizens is central to the deterrence of such attacks and hence to a nation's long-term survival and prosperity. An acknowledged ability to track and trace both domestic and international attackers can preempt future attacks through fear of reprisals such as criminal prosecution, military action, economic sanctions, and civil lawsuits….
>
> The anonymity enjoyed by today's cyber-attackers poses a grave threat to the global information society, the progress of an information-based international economy, and the advancement of global collaboration and cooperation in all areas of human endeavor.[49]

Technical difficulties must be addressed by international standards setting bodies. The TCP/IP protocol,[50] which is the current standard protocol for network communications, seriously limits the ability to track and trace cyber attacks.[51] At present, "the Internet has no standard provisions for

[49] Lipson at 3, http://www.cert.org/archive/pdf/02sr009.pdf.
[50] TCP/IP (Transmission Control Protocol/Internet Protocol). Lipson at 5, http://www.cert.org/archive/pdf/02sr009.pdf.
[51] Lipson at 5, http://www.cert.org/archive/pdf/02sr009.pdf.

tracking or tracing the behavior of its users."[52] Because the Internet protocols were designed for a trustworthy community of researchers, it is quite easy for users to hide their tracks, making it difficult to trace the communications path. For example, because there typically is no capability for cryptographic authentication of the information in IP packets, the information in the packet can be modified and the source address can be forged. "Packet laundering" involves compromising intermediate hosts along a communication path and hopping from host to host such that traceback attempts can be effectively thwarted.[53] These vulnerabilities could facilitate, or disguise, state-sponsored cyber activities or intentionally redirect a cyber criminal act to make it appear that it came from a nation state.

As noted by CERT/CC's Howard Lipson:

> It is clear that tracking and tracing attackers across a borderless cyber-world, and holding them accountable, requires multilateral actions that transcend jurisdictions and national boundaries. Tracking and tracing requires cooperation encompassing the legal, political, technical, and economic realms.…
>
> One of the most significant policy implications of the technical approaches to tracking and tracing… is the need for intense international cooperation at a deeply technical level. This cooperation must go well beyond simple agreements in principle to share tracking data.[54]

Present legal regimes are ineffective in deterring highly relevant threat scenarios that may violate international peace and security. Actions that are prohibited by nation states or considered terrorist or rogue acts against other countries require further deliberation by the United Nations. Internationally agreed standards of conduct are necessary if the Internet is to remain a backbone of economies and a primary means of global communication. In a thorough analysis of the uncharted waters in the area of cyberspace attacks, three renowned scholars in the field argue that:

> In particular, the status of information operations as "force" or "armed attack" is undetermined, an uncertainty which complicates diplomatic and military decision-making. In terms of the UN Charter, it is clear that a range of information attacks would constitute uses of force, and a comparable range of countermeasures would constitute legitimate self-defence….
>
> Beyond these preliminary conclusions, there is far more work to be done on both international technical and legal fronts. Nations that choose to employ information operations, or that expect to be targeted by them, should facilitate tracking, attribution and transnational enforcement through multilateral treaties and, more broadly, by clarifying international customary

[52] *Id.* at 13.
[53] *Id.*
[54] *Id.* at 47.

law regarding the use of force and self-defence in the context of the UN Charter and the laws of armed conflict.[55]

Several scenarios support this conclusion and range from "cyber activists" to information and cyber warfare. On the less serious end of the spectrum, there is the April 1998 distributed denial of service attack launched against the U.S. Department of Defense by "cyber activists" who caused some Department computers to crash.[56] At the other end of the spectrum are direct attacks against the critical infrastructures of one nation state by another. One of the first examples of this was seen in 1991 in Operation Desert Storm when the U.S. disabled Iraq's communications network. Other examples of cyber warfare could include:

- "Means for highly accurate spotting of electromagnetic equipment and its destruction by way of rapid identification of separate components of control, recognition, guidance and fire information systems.

- Means for hitting components of electronic equipment and power supply thereof with a view to putting individual components of electronic systems out of action for short-term or irreversibly.

- Means for affecting data transmission processes with a view to terminating or disorganizing operations of data exchange subsystems, by affecting signal *propagation* environments and functioning algorithms.

- Propaganda and disinformation facilities for modifying control system data, creating a virtual picture of the situation different from the real one, changing human value systems, damaging morale of the adversary's population."[57]

- Packet inspection and modification or rerouting through platform technologies at country gateways.[58]

In between, lay the acts of terrorists or rogue actors that can be equally destructive, as noted in the Introduction to this Report.[59]

Increasingly, nation states, either individually or collectively, are acting to protect their own networks. The range of actions that are possible is considerable, and some can have broad impact on the global network and communications capabilities. It is becoming increasingly clear that companies and countries alike must shift from the reactive mode to the active mode in dealing with cyber attacks. As noted by two World Federation of Scientists experts, "governments (and companies) need the ability to block distributed denial of service attacks, viruses and malicious worms, and protect super-critical and critical infrastructure at the core network level *before* they inflict their damage along backbone

---

[55] Gregory D. Grove, Seymour E. Goodman, and Stephen J. Lukasik, "Cyber-attacks and International Law," *Survival*, Vol. 42, No. 3, Autumn 2000 at 100, http://survival.oupjournals.org/cgi/content/abstract/42/3/89 (hereinafter "Grove, Goodman, and Lukasik").
[56] *Id.* at 90.
[57] Tsygichko at 5-6, http://www.itis-ev.de/infosecur.
[58] Westby and Barletta Consequence Management at 9, http://www.itis-ev.de/infosecur.
[59] *See also* Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters*, Spring 2003, pp. 112-23.

and customer links."[60] An international discussion and understanding regarding what types of proactive actions are acceptable or allowable is necessary to ensure one nation's protective actions do not unduly hinder the communications capabilities of other nations.

The international legal framework is especially murky in the area of cyber attacks and information warfare. The UN Charter was not drafted with the information age in mind and definitions lack clear meaning in the cyber context. The Charter, for example, forbids "acts of aggression" and limits the "threat or use of force" in peacetime. Article 41 grants the Security Council the power to enforce these Charter restrictions through the "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations." Article 42 allows for action by "air, sea or land forces" as necessary to maintain or restore peace. According to one analysis, "Factors that may influence whether something is an act of force include expected lethality, destructiveness and invasiveness."[61]

Thus, Article 41 may be interpreted as allowing some interruption of communications, if it is not done in a manner that is not lethal, destructive or invasive, but what does that mean in the cyber sense? Certainly, some acts against communication systems could be considered quite destructive and/or invasive, such as the manipulation of dam controls or power grids.[62] One of the preeminent authors in this area, Walter Sharp, argues that manipulations or attacks that cause an economic crisis could be deemed a "use of force."[63] And while one action, such as packet sniffing, rerouting, or content modification, may not be lethal or destructive, a reasonable argument can be made that it would be invasive.

Responses to attacks on information systems could conceivably be allowed under Article 51 of the UN Charter, which allows states to take actions in self-defense but requires them to report such actions.[64] Individual responses by states could be either overt or covert, making the reporting requirement problematic in instances of covert actions. Indeed, what types of responses might be acceptable under Article 51 is vague. Moreover, nations could engage in individual or collective cyber self-defense through NATO or other multinational alliances.[65]

The laws of armed conflict must also be factored into any discussion regarding cyber activities of nation states. In times of war, civilian assets that support the military (such as communication systems) may be attacked in order to obtain submission of the enemy, provided that it is limited to military objectives and civilian losses are proportional to the military advantage to be gained – and provided it avoids unnecessary suffering. Possible pre-emptive actions must be also be considered and under what circumstances these might be allowed.[66]

Elaborating upon this nutshell-identification of problems, Andrey Krutskikh, reflecting a general line of thinking among Russian experts, has made a number of suggestions for further international law

---

[60] Westby and Barletta Consequence Management at 8, http://www.itis-ev.de/infosecur.
[61] Grove, Goodman, and Lukasik at 93, http://survival.oupjournals.org/cgi/content/abstract/42/3/89.
[62] *Id.*
[63] *Id.* (citing Walter G. Sharp, Sr., *Cyberspace and the Use of Force*, Aegis Research, Falls Church, VA 1999, at 102).
[64] *Id.* at 95, Timothy L. Thomas (with Karen Matthews), "The Computer: Cyber Cop or Cyber Criminal?" http://www.itis-ev.de/infosecur.
[65] Westby and Barletta Consequence Management at 8.
[66] Grove, Goodman, and Lukasik at 94, 97-100, http://survival.oupjournals.org/cgi/content/abstract/42/3/89.

work that would aim at including cyberattacks more broadly into extant international law. They can be summarized as follows:

- In line with the concept[67] of defining techniques of interfering with information security as "information weapons," despite the present uncertainty on their scope, it is suggested that new, extended criteria for the definition of weapons and armed aggression should be sought, giving emphasis to the objectives of the "aggressor," such as seeking military superiority.[68] Cyber attacks on other states could then be considered acts of armed aggression under 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.

- Further along these lines, the author proposes to establish a list of key information systems of critical relevance for national security which, as a "zone protected by international law," would benefit of protective mechanisms, such as legitimate international emergency responses, beyond the normal rules and practices on reprisals and responses. In the list, a distinction should be made between civilian and transnational facilities, and military systems which may be subject to legitimate attacks.

- On the argument that "cyber weapons" are not currently subject to international treaties pertaining to arms control, Dr. Krutskikh advances several suggestions on a negotiated adaptation of extant treaty law designed to curb the proliferation of such weapons and providing a clear legal framework relating to the aggressive use of cyber operations.[69]

- In an even broader sweep, Dr. Krutskikh, following from earlier official projects within the UN and bilateral diplomacy, develops the idea of a comprehensive international legal regime banning the development, production and use of the "most hazardous types of cyber weapons"[70] for which the key ideas are spelled out in catalogue form.[71] Part of this broad approach is the establishment of an "early warning system." The author also advocates a sanctuary concept under which "global information systems" would be defined and protected as demilitarized zones.[72]

Clearly, the types of cyber activities nation states may engage in, either defensively or offensively, deserve deeper discussion in a multinational forum. The PMP supports the following conclusion:

> As electronic information networks expand and military and industrial infrastructures become more dependent on them, cyber-attacks are bound to increase in frequency and magnitude. Interpretations of the UN Charter and

---

[67] Andrey V. Krutskikh, "International Information Security and Negotiations," Mar. 2003 at p. 3-4, http://www.itis-ev.de/infosecur(hereinafter "Krutskikh"); *see also* Tsygichko, http://www.itis-ev.de/infosecur.
[68] Krutskikh at 3, http://www.itis-ev.de/infosecur.
[69] Krutskikh at 9-11, http://www.itis-ev.de/infosecur.
[70] Joint US-Russia Statement on Common Security Challenges at the Threshold of the 21st Century, Seventh Clinton-Yeltsin Summit, Sept. 2, 1998, http://www.ceip.org/files/projects/npp/resources/summits7.htm#security; Krutskikh at 14-15, http://www.itis-ev.de/infosecur.
[71] Krutskikh at 25, http://www.itis-ev.de/infosecur.
[72] *Id.* at 29.

> of the laws of armed conflict will have to evolve accordingly in order to accommodate the novel definitions of the use of force that such attacks imply….
>
> In terms of the laws of armed conflict, the potentially dangerous consequences of an unnecessary response, a disproportional response or a mistakenly targeted response argue for keeping a human being in the decision loop.
>
> Beyond these preliminary conclusions, there is far more work to be done on both the international, technical, and legal fronts. Nations that choose to employ information operations, or that expect to be targeted by them, should facilitate tracking, attribution, and transnational enforcement through multilateral treaties and, more broadly, by clarifying international customary law regarding the use of force and self-defence in the context of the UN Charter and the laws of armed conflict.[73]

Operationally, scientific studies and scenario generation exercises should be undertaken in the international legal and technical communities, involving the General Assembly and First and Sixth Committees. The International Law Commission could be tasked with developing an appropriate legal framework defining legitimate cyber actions by nation states.

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

Ordering cyberspace under the perspective of universality requires comprehensive involvement by the United Nations. In many ways, this challenge has already been recognized and is increasingly met by various UN offices and bodies as well as by members of the wider UN family. There are also global initiatives undertaken by the private sector that purport to work towards similar ends and could usefully be included in an over-all effort.

These manifold, widely dispersed efforts are, however, difficult to follow and to assess in their overall impact. A central focal point within the UN itself could perform a coordinating, evaluating, and synthesizing function. Without prejudice to the mandate or autonomous policy decisions of other UN branches or outside organizations, such a forum could catalogue and assess the work done elsewhere, point to inconsistencies and duplication, identify gaps and new research requirements, and stimulate coordinated approaches.

The problem is far wider than just a question of the Digital Divide.

The list of UN or UN-related actors in the field is already long. Apart from a number of resolutions adopted by the General Assembly, the UN ICT Task Force, UN Institute for Training and Research

[73] Grove, Goodman, and Lukasik at 100, http://survival.oupjournals.org/cgi/content/abstract/42/3/89.

(UNITAR), the UN Center for Social Development and Humanitarian Affairs, the UN Committee on International Trade Law (UNCITRAL), the UN Conference on Trade and Development (UNCTAD), and the UN Office for Drug Control and Crime Prevention have provided inputs in their particular field of action. Other UN entities such as the World Intellectual Property Organization (WIPO), the International Telecommunications Union (ITU), and the International Atomic Energy Agency (IAEA) have made contributions, as have the International Organization for Standardization (ISO), the International Civil Aviation Organization (ICAO), the International Air Transport Association (IATA), and others.

From the private sector, activities with a global perspective are undertaken, among others, by the International Chamber of Commerce (ICC), the Global Business Dialogue on Electric Commerce (GBDe), the World Information Technology and Services Alliance (WITSA), the Global Internet Project, the Global Information Infrastructure Commission (GIIC), and the Information Technology Association of America (ITAA).

The special UN forum recommended here should, of course, also take cognizance of the ongoing work undertaken by the OECD (especially its recently updated *Guidelines for the Security of Information Systems and Networks*), the G8, the European Community, and the Council of Europe.

Given the broad scope of cyberspace related problems, the forum would be best established as a special entity within the UN Secretariat or as body reporting to the UN General Assembly. Mechanisms should be developed to incorporate all stakeholders in the work of such a body.

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.**

The above list of possible attributions for the intended Agency appears to be self-explanatory and sufficient to set in motion the process of examining its feasibility. The Agency is perhaps best established within the UN system, but an institutional format on the basis of public-private partnership is not to be excluded. The PMP is mindful of current UN budget constraints and the general reluctance of governments to embark on new institutional solutions. However, given the amount of work already performed in various bodies, UN and others, in the IT field, the organization chart of the Agency could be small, and some reshuffling of personnel might be possible. The point is to create a central entity that can serve as a clearinghouse and coordination center for the various initiatives and work already undertaken or developed in this area. The initiative for a feasibility study might usefully be taken by the UN Secretary General.

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.

Rapid innovations of ICTs and the development of a wide variety of ICT products and applications has resulted in a permanently increasing and heterogeneous ICT-user community of all ages, skills, and intellectual and cultural backgrounds. ICT products are becoming more and more pervasive and ubiquitous resources of our life. More or less, all individuals use ICT products as part of their private, professional, and public life. ICTs are becoming such a part of everyday life, we are becoming as accustomed to using them as we are with other natural or technical resources.

With respect to this situation, all individuals have to become aware of not only the advantages of ICT applications, but also of their consequences and – sometimes hidden – risks, especially concerning safety and security. Making people aware of the risks associated with ICTs requires, at first, the development of an educational framework, and of easily accessible information systems and sources, which provide individuals with information and knowledge about data and information security risks according to their individual background, skills, and needs:

- All individuals should at least have a basic understanding of the key information security properties of an ICT system, like confidentiality, data integrity, user authentication, and access control mechanisms.

- All ICT users also have to understand that besides risks for their privacy, other risks may exist for their local environment, for a larger community, or even for the public.

- Adequate information about technical attacking techniques (e.g. viruses, trojan horses), and of non-technical attacking possibilities (e.g. social engineering)[74] should be widely available to the public.

- An educational program should include some general procedures for intrusion prevention, intrusion detection, damage analysis, and recovery mechanisms.

- All educational curricula must incorporate codes of ethical conduct for ICT activities and begin at the primary school level and extend through secondary and tertiary levels and be incorporated into training programs in the workplace, community centers, and other venues for individual citizens.

The ISO Code of Practice for information security defines the 10 guiding principles which should be considered and presented to all ICT users according to their individual needs, skills, and background.[75]

Along the same lines, the UN publication *Information Insecurity: a survival guide to the unchartered territories of cyber-threats and cyber-security* presents a detailed description of the information security problems we have to face, and it includes all relevant information for prevention and actions. Together, with the cited sources and examples, it forms an excellent framework and source for assembling educational programs as discussed above. Numerous other organizations have compiled valuable materials in this area.[76]

To provide all kinds of users with the required input on information security issues, educational curricula, as well as decision support and advisory information, this content should be distributed not only by printed articles and books, but also by the use of new media, ICT products, and/or the Internet. For example, educational curricula can be utilized in teleteaching and intelligent tutoring systems, enabling students to learn about this subject independent of time and location. Another technical approach could offer information security expertise via information bases, or knowledge bases, via an expert system interface. The expert system interface could be adapted according to a user's requirements, or skills, thus enabling goal-directed access to information and expertise.[77]

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

---

[74] Social engineering refers to the false representation that one has system administration authorities with the intention of luring the system user into revealing critical authorization or access controls, or similar types of deceptive behavior that enables an unauthorized user access to information or infrastructure.

[75] *See* e.g., "International Standard ISO/IEC 17799: 2000 Code of Practice for Information Security Management, Frequently Asked Questions," Nov. 2002, http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf.

[76] Gelbstein and Kamal, http://www.un.int/kamal/information_insecurity; *see e.g.*, Westby Cybercrime at 161-70, http://www.abanet.org/abapubs/books/cybercrime/; Jody R. Westby, ed., *International Strategy for Cyberspace Security*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, to be published fall 2003.

[77] *See also* Axel Lehmann, "Heightening Public Awareness and Education on Information Security," http://www.itis-ev.de/infosecur

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.

Corporate directors and officers have a fiduciary duty of care to protect corporate assets. Since an estimated 80 percent of corporate assets today are digital,[78] it logically follows that oversight of information security falls within the duty owed by officers and directors in conducting the operations of a corporation. Today, it is increasingly clear that officers and boards of directors have a corporate governance responsibility with respect to the security of company data, systems, and networks. Hacking, denial of service attacks, economic espionage, and insider misuse of data and systems are commonplace and threaten the profitability of every business, leaving officers and directors vulnerable to lawsuits and civil and criminal penalties.

To date, no shareholder suit has been brought against officers or directors for failure to take necessary steps to protect corporate systems and data, however, shareholders may have a valid basis for such derivative suits.[79]

The majority of U.S. jurisdictions follow the business judgment rule that the standard of care is that which a reasonably prudent director of a similar corporation would have used. The recent Delaware case, *Caremark International Inc. Derivative Litigation*, held that, "a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under certain circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards."

The recent *Caremark* case noted that officer/director liability can arise in two contexts: (1) from losses arising out of ill-advised or negligent board decisions (which are broadly protected by the business judgment rule so long as the decision was reached out of a process that was rational or employed in a good faith effort) and (2) from circumstances where the board failed to act in circumstances where "due attention" would have prevented the loss. In the latter situation, the *Caremark* court noted that:

> [I]t would, in my opinion, be a mistake to conclude that . . . corporate boards may satisfy their obligation to be reasonably informed concerning the corporation, without assuring themselves that information and reporting systems exist in the organization that are reasonably designed to prove to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance. . . .
>
> Obviously the level of detail that is appropriate for such an information system is a question of business judgment. . . But it is important that the board exercise a good faith judgment that the corporation's information and

[78] "Cybercrime," *Business Week*, Feb. 21, 2000.

[79] Jody R. Westby, "Protection of Trade Secrets and Confidential Information: How to Guard Against Security Breaches and Economic Espionage," *Intellectual Property Counselor*, (Jan. 2000) at 4-5.

> reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.
>
> *Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

The *Caremark* case could provide a basis for a shareholder suit against officers and directors of U.S. companies for failure to implement an information and reporting system on the security of corporate networks and data such that it could (1) determine it is adequately meeting statutory, regulatory, or contractual obligations to protect certain data from theft, disclosure or inappropriate use and (2) be assured that the data critical to normal business operations, share price, and market share is protected.[80]

There are also high risk situations where higher standards apply to directors and officers, such as acquisitions, takeovers, responses to shareholder suits, and distribution of assets to shareholders in preference over creditors. In these circumstances, directors and officers are required to obtain professional assistance or perform adequate analyses to mitigate the risks that ordinarily accompany these activities. Some information assurance experts assert that a "higher degree of care will also be required of Directors and Officers regarding the complex nature of issues involved in information assurance."[81]

Securities laws and regulations require public corporations to adequately disclose in public filings and public communications relevant risks to the corporation and its assets. The U.S. Sarbanes-Oxley Act requires management's attestation that information assets are protected. Additional exposure is caused by insurance companies now routinely excluding hacking and IT-related incidents from general liability policies. Also, senior management in certain industry sectors may be subject to civil and criminal penalties for inadequate security and privacy of protected classes of data. And legal actions continue to mount against corporations for security and privacy breaches. The *Independent Director* put this in the context of information systems by reporting that:

> Management of information risk is central to the success of any organization operating today. For Directors, this means that Board performance is increasingly being judged by how well their company measures up to internationally-accepted codes and guidelines on preferred Information Assurance practice.[82]

Additionally, when an organization is a victim of an attack on its information systems, whether from an insider or an outside bad actor, previous studies have shown that this can result in a lack of

---

[80] *See, e.g., id.*; For a general discussion on corporate liability related to board and officer responsibilities to ensure adequate information and control systems are in place, *see* Steven G. Schulman and U. Seth 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, http://www.plusweb.org/Events/Do/materials/2002/Source/Duties%20and%20Liabilities.pdf.

[81] Dr. John H. Nugent, CPA, "Corporate Officer and Director Information Assurance (IA) Liability Issues: A Layman's Perspective," December 15, 2002, http://gsmweb.udallas.edu/info_assurance.

[82] *Id.* (citing Dr. Andrew Rathmell, Chairman of the Information Assurance Advisory Council, "Information Assurance: Protecting your Key Asset," http://www.iaac.ac.uk).

confidence in the company and even a drop in the company stock price.[83] Consequently, shareholders may also initiate a derivative suit for loss to stock price or market share caused by inadequate attention by officers and directors to information security.[84]

According to the SANS Institute, the seven top management errors that lead to computer security vulnerabilities are:

> "1. Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.
>
> 2. Fail to understand the relationship of information security to the business problem – they understand physical security but do not see the consequences of poor information security.
>
> 3. Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed.
>
> 4. Rely primarily on a firewall.
>
> 5. Fail to realize how much money their information and organizational reputations are worth.
>
> 6. Authorize reactive, short-term fixes so problems re-emerge rapidly.
>
> 7. Pretend the problem will go away if they ignore it."[85]

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.

Legal action taken in courts and by regulatory agencies and underwriting requirements by insurance companies are pushing civil responsibility for information security. Action taken in multinational fora is also expected to impact corporate liability and officer/director responsibility. Article 12 of the Council of Europe Convention on Cybercrime (CoE Convention) requires signatory states to establish laws that hold companies civilly, administratively, or criminally liable for cybercrimes that benefit the company and were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director. Article 9 of the European Union's

---

[83] A. Marshall Acuff, Jr., "Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business," Salomon Smith Barney, 2000, at 3-4, http://www.ciao.gov/industry/SummitLibrary/InformationSecurityImpactingSecuritiesValuations.pdf.

[84] Much of this section was taken from: Jody R. Westby, ed., *International Strategy for Cyberspace Security*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, to be published fall 2003.

[85] "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities," The SANS Institute, http://www.sans.org/resources/errors.php.

proposal for a Council Framework Decision on attacks against information systems mirrors the CoE language.

These provisions have been cited as an example of emulation for a broader international constituency in light of the need to be adapted for insertion into the new Model Law on Cyberspace.

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.

The concept of "open source" is now getting wide attention from a global community of users and developers. Open source does not refer to the price of software; it may be distributed free of charge or for a fee. The concept of open source or "free software" lies in the freedom associated with the code. This freedom, however, is contained within set limitations. An open source license[86] provides freedom to any programmer to use the code, but defines the social parameters programmers must observe regarding the code. Open source generally means that:

1. The software is developed by a community of programmers, usually from around the globe.

2. The source code is distributed or easily available either without charge or for a minimal fee.[87]

3. Improvements, changes, and corrections may be made to the software, but these must also be freely distributed without attempt to "privatize" the program. The license may require the source code to be distributed separately from modifications contained in "patch files," it may completely restrict distribution of modified source code, or it may require derived works to be distributed under a different name or version number from the original.

4. The copyright is held by the original author(s).

5. The rights attached to the program must apply to all to whom the program is distributed, without restriction that it be used for only a certain business, etc. or without restriction that any other software distributed with the program need be open source.

6. The license must be technology neutral.[88]

---

[86] *See* http://www.opensource.org/licenses/ for access to an array of approved open source licenses.
[87] The Open Source Initiative requires free distribution, although a license "shall not restrict any party from selling or giving away the software….The license shall not require a royalty or other fee for such sale." Open Source Initiative, The Open Source Definition, http://opensource.org/docs/def_print.php.
[88] David McGowan, "Legal Implications of Open-Source Software," Univ. of Ill. Law Rev., Vol. No. 1 2001 at 241 (hereinafter referred to as "McGowan"); The Open Source Definition, Version 1.9, Open Source Initiative, http://opensource.org/docs/def_print.php. Open source licenses are not consistent in intent and meaning of traditional software licenses and have not been tested in court. *Id.* at 243.

In a nutshell, open source can generally be referred to as "an approach to software development with unique licensing arrangements and a community-based method of programming."[89] A reverse concept from commercial software licenses that restrict distribution, sale, modification, use, etc., open source provides the global community of programmers access to source code and provides "freedom" to work within a community of accepted norms with respect to how that software code is handled, modified, distributed, used, etc.[90]

Because the term "open source" is a descriptive term, it cannot be protected by a trademark. Therefore, in order to "mark" software that is distributed under a license that conforms to the Open Source Initiative (OSI) definition, the OSI has registered a certification mark "OSI Certified" for this single purpose and has created a graphical certification mark for it. OSI maintains a list of registered licenses.[91]

The Linux operating system is perhaps the best known open source software example. Apache, BIND, Netscape, and GNU Linux which is the open source program for Red Hat, are others.[92] The OSI definition and its certification mark are not only applicable for software programs, but also for firmware programs offering an application-oriented usage of microprocessors, and of digital control and processing units (e.g., by means of Read-only Memory (ROM's)).

An open source approach is not as easily applied to hardware. There is no standardized definition and understanding available for open source hardware, as there is for software or firmware. One obvious reason lies in the lack of an easy or inexpensive method for copying hardware, such as exists for software or firmware programs. However, in 1997, some ICT hardware manufacturers formed an Open Hardware Certification Program as a self-certification program for hardware manufacturers whose hardware is Linux or FreeBSD ready.[93] Hardware with an HDL-specified hardware description (which means that a hardware device is precisely specified by a Hardware-Description-Language program) enables easy copying and distribution of the hardware's specifications, but not of the hardware itself.[94]

With respect to ICT security considerations, open source or OSI certified programs could function in the marketplace to provide increased confidence in commercial off-the-shelf (COTS) products by providing:

- An approved license;
- A complete and certified description of the software or firmware and its functionalities or operations; and

---

[89] Dennis M. Kennedy, "A Primer on Open Source Licensing Legal Issues: Copyright, Copyleft and Copyfuture," at 1, http://www.denniskennedy.com/opensourcedmk.pdf (hereinafter "Kennedy").
[90] McGowan at 244-45, http://opensource.org/docs/def_print.php; Kennedy at 3-4, http://www.denniskennedy.com/opensourcedmk.pdf.
[91] OSI Certification Mark and Program, Open Source Initiative, http://opensource.org/docs/certification_mark.php.
[92] McGowan at 241, http://opensource.org/docs/def_print.php; Kennedy at 1, 9 http://www.denniskennedy.com/opensourcedmk.pdf.
[93] Open Hardware Certification Program, http://www.open-hardware.org/.
[94] Richard Stallman, "Free Hardware," http://features.linuxtoday.com/news_story.php3?ltsn=1999-06-22-005-05-NW-LF.

- An understanding of its compatibilities and implementation.

From the COTS developers' point of view, however, traditional, commercially licensed software can have market advantages over open source. From the customer's point of view, open source enables a product's user to adjust, refine, adapt, or enlarge the product coincident with its specification and according to the customer's specific requirements.

The open source movement is gaining momentum, especially in developing countries where governments and businesses chafe against high license fees for Microsoft and other proprietary software products. The movement is still relatively young and refinements, as well as additional quality measures and specification standards, are certain to follow.

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.

In addition to action taken in the UN and the Council of Europe, activities regarding information security and cybercrime should proceed in other fora, including regional and multilateral organizations and meetings. Regional efforts consistent with the global developing legal framework are encouraged. Regional activities are often very productive because consensus is easier to reach within regional organizations and linkages are typically stronger than those in international fora. Additionally, certain actions that would promote information security and a harmonized global legal framework would be appropriate for discussion in the World Trade Organization Doha Round.

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.

Disparities in the international legal environment greatly handicap law enforcement activities and often make it impossible to proceed in investigating cybercrime cases and bringing the perpetrators to justice. The speed and flexibility of cyber attacks (they can take place in an instant, or can be spread out over extended periods of time in a "low and slow" attack scenario that can be very difficult to detect) pose significant legal challenges to our traditional law enforcement environment. Particularly vexing legal issues include, but are not limited to: intercepting communications, searching and seizing electronic evidence, differing requirements for archiving logs of transactions and traffic generated at computer and communication systems, obtaining information from communication and Internet service providers, and ensuring validity of cybercrime evidence across a variety of legal jurisdictions. International law enforcement initiatives can leverage national efforts and create momentum for change.

The EU has addressed the cooperation of international law enforcement with respect to cybercrime through the European Police Office (Europol).[95] Headquartered in The Hague, The Netherlands, Europol is the EU's law enforcement organization responsible for improving the effectiveness and

[95] *See* Europol's website at http://www.europol.eu.int/home.htm.

cooperation between competent authorities in EU Member States. It was established on February 7, 1992, under the Treaty on European Union and is accountable to the Council of Ministers for Justice and Home Affairs. Europol became fully operational on July 1, 1999. Its mandate includes preventing and combating terrorism, drug trafficking, and other serious forms of international organized crime, such as immigration networks, vehicle trafficking, trafficking in human beings including child pornography, forgery of money and other means of payment, money laundering, and trafficking in radioactive and nuclear substances.

Europol has approximately 250 members on staff, all of whom have been assigned by various EU member nations. Approximately 45 of these staff members – known as Europol Liaison Officers (ELOs) – represent their nation's various law enforcement agencies such as police, customs, gendarmerie, and immigration services.[96] Europol recently completed the phased deployment of The Europol Computer System (TECS). The new computer system is specifically designed to facilitate the sharing and analysis of criminal data between EU member nations and law enforcement organizations in other countries. Each EU member nation has assigned two Data Protection Experts to Europol to closely monitor how personal data is stored and used.

In September 2000, the EU's Council of Ministers for Justice and Home Affairs asked EU member nations to start responding to requests from Europol to investigate specific cases, and keep Europol informed about the status and results of the investigation. Since November 2000, EU member nations have been able to leverage the resources of Europol National Units (ENUs) on joint investigations in accordance with the *Europol Convention*[97] and its implementing rules. The European Police Chiefs Operational Task Force[98] coordinates its activities with Europol in combating transnational crime.

The International Criminal Police Organization (Interpol) was founded in 1923 and has been located in Lyon, France since 1989. Interpol is an important link among law enforcement organizations globally.[99] Interpol has 178 member countries and maintains close working relationships with dozens of intergovernmental bodies such as the Council of Europe and World Customs Organization. Interpol's primary mission is to promote the widest possible mutual assistance between all criminal police authorities.

Interpol has a system of offices around the world referred to as National Central Bureaus (NCBs). Each of its 178 member nations has an NCB station, generally within that nation's capital. One or more local law enforcement agencies are responsible for staffing the NCB and represent national law enforcement to Interpol. For example, in Canada, the Royal Canadian Mounted Police (RCMP) staff and support the NCB in Ottawa. Should a police officer in Montreal or Winnipeg need something from the police in Gaberone, Botswana, the Montreal police would route their request through their police computer systems to the NCB in Ottawa. The RCMP staff would then forward that request via a private encrypted computer network to the Interpol Secretariat General in Lyon, France. The bureau receiving the message at the Secretariat would read the message and forward it to the

[96] *See* http://www.europol.eu.int/content.htm?links/en.htm for links to EU Member States' national law enforcement websites, links to European institutions and international organizations, and links to other law enforcement agencies and organizations.
[97] The text of the *Europol Convention* can be found at http://www.europol.eu.int/content.htm?legal/conv/en.htm.
[98] *See* http://www.eurunion.org/partner/EUUSTerror/PoliceChiefsTaskForce.htm for more information on the European Police Chiefs Operational Task Force.
[99] *See* Interpol website at http://www.interpol.int/.

necessary agency in Botswana. Each of the 178 countries participating in the Interpol system has access to special computer and telephone systems to facilitate the transfer of this information.

Interpol has been actively involved in combating Information Technology Crime (ITC) for a number of years. The Interpol General Secretariat has harnessed the expertise of its members in the field of ITC through "working parties" or groups of experts. Each working party consists of the Heads or experienced members of national computer crime units. Working parties are designed to reflect regional expertise and are established in Europe, Asia, the Americas, and Africa, although each is in different stages of development. In addition, Interpol has created several handbooks and computer crime manuals that it distributes to law enforcement agencies worldwide to use as best practice guides. Interpol currently has a number of ongoing projects related to high technology crime, including information sharing mechanisms for law enforcement and a 24 hour/7 day a week point-of-contact network to allow investigators in one jurisdiction to locate and communicate with their counterparts abroad.[100]

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.

Increasingly, we realize that the globally connected network is a multidisciplinary effort that combines scientific and technological achievements with legal and policy considerations. Over the past few years, a legal and policy framework has developed that, in large part, is responsive to both the capabilities of networked communications and the vulnerabilities of Internet protocols, software, and networks. The ability of governments and private sector entities to access, gather, and retain vast amounts of information about Internet users has raised concerns of privacy groups, consumer advocates, and civil libertarians. Likewise, they have also been alarmed by government use of the Internet and ICTs in national and global surveillance and their potential government access to Internet account and traffic data.

To date, there has been little interaction and coordination between the scientific and technological communities and the legal/policy community. While generally aware of each other's endeavors, there has been minimal effort to identify critical intersection points to engage in multidisciplinary initiatives to resolve critical information security problems. It is incumbent upon the scientists and technologists to bring together stakeholders from the legal and policy realms to explain the capabilities and vulnerabilities of ICTs and to begin a dialogue to bridge the gaps in understanding. For example, legislators and policymakers are currently developing privacy and security laws, often without a clear understanding of whether they are actually addressing the issues caused by technological weaknesses and vulnerabilities or merely papering over a problem area.

[100] *See* http://www.interpol.int for further information on Interpol. Much of the commentary to this Recommendation was taken from the Law Enforcement Chapter of the *International Guide for Combating Cybercrime*, which was co-authored and edited by Jody Westby. *See* Westby Cybercrime at 95-98, http://www.abanet.org/abapubs/books/cybercrime/.

A. Technologies With Significant Legal and Policy Implications

1. Encryption, Signatures, and Authentication

Cryptography has become an integral part of seeking to assure an acceptable level of security and privacy of communications and data storage. The development and use of sophisticated, strong cryptography has a long history as a technique used by governments to protect sensitive information. The development of public key cryptography[101] in 1975, and the subsequent evolution of that approach have put strong cryptography in the hands of private enterprises and the general public. Today, research and development into increasingly stronger, more efficient, and widely-usable encryption techniques continues at a high level.

For years, legal and policy conflicts swirled around the public use of strong encryption technologies. The U.S., in particular, tried to regulate public use of encryption and the export of low-level encryption technologies and pushed legislative agendas mandating key escrow or embedded chips, arguing law enforcement would be stymied without such controls. Fierce resistance by industry, academia, scientists, technologists, and policymakers ultimately defeated these efforts and the unregulated public use of encryption became the global standard.

Today, only a few countries regulate public use of encryption, although many countries control the export of powerful, dual-use encryption technologies. A few countries, such as the U.K., require assistance with decryption or demand the encryption key be given to law enforcement upon request.[102] Overall, governments around the globe have concluded that the benefits of encryption outweigh the negative consequences of encrypted communications by criminals. As lawmakers moved away from controlling encryption, their understanding of the importance of information security resulted in the enactment of laws and regulations that promote the use of authentication and authorization technologies.

There is little understanding, however, outside the scientific and technical communities regarding the capabilities to decrypt messages either real-time or offline. As more evidence mounts that Al Qaeda terrorists are using encryption technologies to protect their communications,[103] the old fears surrounding encryption begin to surface once more. Because innovations are constantly changing both the state of encryption technologies and the ability to decipher these communications, a continuing dialogue between scientists, technologists, policymakers, and stakeholders is critical.

2. Tracking and Tracing Internet Communications

A technology issue central to deterring cyber attacks on information infrastructures is the degree to which attacks can be tracked to their origin. With the present TCP/IP protocol, there is very little ability to track and trace Internet attacks to their source.[104] For example, information in an IP packet

---

[101] Whitfield Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE, *Transactions on Information Theory*, Vol. IT-22, Nov. 1976 at 644-654.
[102] Westby Cybercrime at 44, 74, http://www.abanet.org/abapubs/books/cybercrime/ (citing *Cryptography and Liberty 2000: An International Survey of Encryption Policy*, Electronic Privacy Information Center, http://www2.epic.org/reports/crypto2000).
[103] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters*, Spring 2003 at 112.
[104] Lipson at 5, 13, http://www.cert.org/archive/pdf/02sr009.pdf.

can easily be modified, the source address can be forged, and communications can be woven through intermediary hosts prior to reaching its destination ("packet laundering").[105] The critical link between technology and policy today is succinctly articulated by CERT/CC's Howard Lipson:

> In this high-threat, target-rich environment, the technical ability to reliably track and trace intruders (supported by international agreements on monitoring and information sharing, and by international law proscribing attacks and specifying sanctions and punishment) is an indispensable element for enabling the continued use of the Internet to provide many of the essential services that societies depend on.[106]

Even with an accommodating policy environment, ISPs are likely to require both technical assistance and financial incentives to support tracking and tracing endeavors due to the cost and burden they impose on their operations.

Emerging next-generation standards and protocols from the Internet Engineering Task Force (IETF) promise to enable improved security and significantly greater tracking and tracing of cyber-attacks. IPsec is an emerging security standard for IP that provides for packet authentication and confidentiality and can be used to cryptographically authenticate a packet's source address. The Internet Protocol Version 6 (IPv6) is the next generation standard protocol that is slowly replacing the current version, which is IPv4. The security features of IPsec are made available in every IPv6 implementation, although the use of IPsec features is optional. Moreover, IPv6's expanded header size can enable more tracking and audit data to be stored. Its increased address space would make it possible (though not a requirement) for every network device to be assigned a static IP address, making it easier to link a particular IP address with an entity or individual. The adoption of IPv6 by the user community is proceeding slowly, however, due to high conversion costs.[107]

Most tracking and tracing approaches are only effective against attacks that generate large floods of attack packets. However, there is promising ongoing research focused on the capability to track even single attack packets to their source. Such a tracking capability would require the storage, for some limited time, of a digest of all packets seen by participating routers. This would require very large data storage resources, even if only a small fraction of each packet is retained. Such large-scale storage has significant privacy implications, and is clouded with jurisdictional, legal, and law enforcement considerations.[108]

Thus, the dialogue between scientists, technologists, and policymakers is all the more critical during this time of transition when cyber attacks are on the rise and our ability to track and trace them is limited. Howard Lipson wisely notes:

> The ability to accurately and precisely assign responsibility for cyber-attacks to entities or individuals (or to interrupt attacks in progress) would allow society's legal, political, and economic mechanisms to work both domestically and internationally, to deter future attacks and motivate evolutionary

[105] *Id.* at 13-15.
[106] *Id.* at 16.
[107] *Id.* at 60-61.
[108] *Id.* at 43.

> improvements in relevant laws, treaties, policies, and engineering technology….
>
> However, improvements to current Internet technology, including improved protocols, cannot succeed without an in-depth understanding and inclusion of policy issues to specify what information can be collected, shared, or retained, and how cooperation across administrative, jurisdictional, and national boundaries is to be accomplished. Nor can policy alone, with only high-level agreements in principle, create an effective tracking and tracing infrastructure that would support multilateral technical cooperation in the face of attacks rapidly propagating across the global Internet. *To be of value, the engineering design of tracking and tracing technologies must be informed by policy considerations, and policy formulations must be guided by what is technically feasible and practical.* International efforts to track and trace cyber-attacks must be supported by intense technical cooperation and collaboration in the form of a multilateral research, engineering, and technical advisory group that can provide the in-depth technical skill and training to significantly improve the capabilities of incident response teams and law enforcement.[109]

Anonymizer technologies can defeat tracking and tracing capabilities. These technologies are extremely controversial due to their ability to protect privacy on the one hand, while defeating the ability of law enforcement and private sector entities to track and trace attacks and illegal conduct.

3. Response and Recovery Technologies

Despite the theoretical and practical advances in tracking capabilities in the future, the prudent course of action for protecting information infrastructures is to adopt self-healing or self-mitigating architectures and operational procedures that are survivable in the face of sophisticated attacks. Survivability strategies include sophisticated schemes to simulate, detect, and respond to attacks whether from the outside or inside of the system.[110] This area will require continuing technical, legal, and policy collaboration, but the rewards could be rich.

4. Multilateral, Multidisciplinary Technical Research, Engineering, and Advisory Capability

Many nations are beginning to understand that security of cyberspace requires a strategy that is linked to a nation's economic and national security interests. In February 2003, the U.S. released its *National Strategy to Secure Cyberspace.* The Strategy is intended to help the U.S. protect its critical infrastructures and to reduce vulnerabilities that can be exploited in order to "ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least public damage."[111] Other nations are similarly taking a national look at how their public and

---

[109] *Id.* at 63-64 (emphasis added).
[110] Howard F. Lipson and David A. Fisher, "Survivability—A New Technical and Business Perspective on Security," http://www.cert.org/archive/pdf/busperspec.pdf; Westby and Barletta Consequence Management at 9-12 http://www.itis-ev.de/infosecur..
[111] *The National Strategy to Secure Cyberspace*, cover letter from President Bush, Feb. 2003, http://www.whitehouse.gov/pcipb/.

private sectors are securing critical information infrastructures and the relationship between cyber attacks and national and economic security.

Numerous technical information security activities have also been undertaken by the U.S. National Institute of Standards and Technology (NIST), resulting in several government technical standards and criteria for security products. As a forerunner, in 1995, the British Standards Institution developed British Standard 7799, a Code of Practice for Information Security Management. This standard has now been accepted as an international standard, ISO/IEC 17799.[112]

Although international standards setting bodies, such as the IETF and IEEE,[113] have been working closely in the area of cyber security and infrastructure protection for years, there is a lack of multidisciplinary collaboration on technical, legal, and policy issues at the nation state level. The Internet Society (ISOC), the main governing body of the Internet, presently covers some of this ground, but it is an independent, professional membership society comprised of more than 150 organizations and 11,000 individual members from 182 countries. It is not a multinational body of nation states that collectively discusses the array of issues concerned with cyber security and reaches agreements on cooperation, legitimate actions, and penal codes.

It is impossible for any country to *unilaterally* achieve security in a globally connected network environment. Again, CERT/CC's Howard Lipson, recognizes this void:

> Regardless of the precise organizational structure, a *multilateral technical research, engineering, and advisory capability* is essential to (a) research and recommend the best tracking and tracing techniques and practices, (b) provide ongoing support for a multilateral tracking and tracing capability, (c) provide ongoing training and awareness for cooperating incident response and investigatory teams world-wide, (d) make recommendations to international engineering bodies, such as the Internet Engineering Task Force (IETF), for protocol improvements and standards creation in support of member states' requirements for tracking and tracing attackers, (e) interact with those creating cyber-law and policy to ensure that the technical and non-technical approaches complement and support each other, (f) help assure that the tracking and tracing infrastructures and technologies of cooperating entities can interoperate, and (g) assess the results of cooperation already undertaken by technical and law enforcement agencies, in order to provide feedback for continual improvement.[114]

---

[112] ISO/IEC 17799:2000 Information technology -- Code of practice for information security management. http://www.iso.ch/cate/d33441.html.

[113] Internet Engineering Task Force (IETF), http://www.ietf.org; Institute of Electrical and Electronics Engineers (IEEE), http://www.ieee.org.

[114] Lipson, p. 48 (emphasis in original), http://www.cert.org/archive/pdf/02sr009.pdf.

B. Examples of Technologies Engendering Potential Conflict with Human Rights

1. Data mining, profiling and biometric technologies

Of great concern since September 11, are information processing and retrieval technologies aimed at detecting and identifying terrorists from text-based and network-based databases through the identification and tracking of the actions of communities, the prototyping and profiling of suspects groups and individuals, and the matching of keywords, phrases, and patterns of expression. These technologies presuppose the existence of very large searchable databases.

The concern over the excessive use of data warehousing and mining is exemplified by the debate in the U.S. of the Total Information Awareness (TIA) program[115] being promoted by the U.S. Defense Advanced Research Projects Agency (DARPA). According to DARPA, TIA is developing:

> 1) architectures for a large-scale counter-terrorism database, for system elements associated with database population, and for integrating algorithms and mixed-initiative analytical tools; 2) novel methods for populating the database from existing sources, creating innovative new sources, and inventing new algorithms for mining, combining, and refining information for subsequent inclusion into the database; and, 3) revolutionary new models, algorithms, methods, tools, and techniques for analyzing and correlating information in the database to derive actionable intelligence."[116]

DARPA is also developing Human Identification at a Distance (HumanID)[117] which is a suite of automated biometric identification technologies to detect, recognize, and identify humans at great distances.

TIA would monitor the daily personal transactions by Americans and others, including tracking the use of passports, driver's licenses, credit cards, airline tickets, and rental cars. Privacy groups and civil libertarian organizations immediately raised 1984 Orwellian "Big Brother" concerns over such government use of these technologies. The U.S. Congress quickly became involved. Senator Patrick Leahy noted in a letter to U.S. Attorney General John Ashcroft that:

> Collection and use by government law enforcement agencies of such commercial transactional data on law-abiding Americans poses unique issues and concerns, however. These concerns include the specter of excessive government surveillance that may intrude on important privacy interests and chill the exercise of First Amendment-protected speech and associational rights.[118]

---

[115] This system is now being referred to as Terrorism Information Awareness program. *See* "DOD surveillance system renamed, But details of Pentagon data-gathering project unchanged," http://www.stacks.msnbc.com/news/916028.asp.
[116] "Total Information Awareness (TIA) program being promoted by the US Defense Advanced Research Projects Agency (DARPA), http://www.darpa.mil/iao/TIASystems.htm .
[117] "Human ID at a Distance (HumanID)", http://www.darpa.mil/iao/HID.htm.
[118] "Letter to Attorney General John Ashcroft", U.S. Senator Patrick Leahy, January 10, 2003, http://www.senate.gov/~leahy/press/200301/011003.html.

Subsequently, the U.S. Congress has blocked funding for the TIA program.[119] However, this is but one small system out a vast array of government systems around the globe that uses ICTs to monitor, track, and keep information on the activities and movements of people inside their countries. Authoritarian regimes routinely block access to certain Internet sites, and because they are also usually the monopoly provider of communications, they have unfettered access to an array of communication traffic and content data. However, even democracies such as the U.S. have developed sophisticated systems to monitor email traffic. The "Carnivore" system, developed by the FBI, can be installed on an ISP to monitor all traffic moving through that provider. Although the FBI claims the system is designed to "filter" traffic and allow investigators to see only those packets the FBI is lawfully authorized to obtain, privacy and civil liberties groups remain skeptical.[120]

2. Global electronic surveillance

The ECHELON system is an "automated global interception and relay system operated by the intelligence agencies in five nations:" the U.S., U.K., Canada, Australia, and New Zealand, with the U.S. National Security Agency at the helm.[121] A provisional report of the European Parliament confirms that "the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt."[122] The report further confirms that "the purpose of the system is to intercept private and commercial communications, and not military communications"[123] This system and its potential for violating civil liberties of citizens has been the subject of inquiry by the legislatures of the Netherlands, Italy, and the United States among others.[124]

3. Anonymity, privacy, and freedom of expression

Anonymity and privacy are frequently used interchangeably, especially, in colloquial speech. Anonymity, seen as a part of privacy (privacy of identity), can be an important means of preserving international human rights and freedom of expression. Lack of anonymity in an expanding world of information technology makes it increasingly easy for private sector entities (with particular regard to economic interests) to gather vast amounts of information and track Internet activity and for

---

[119] "Terrorism spying project to end: Personal records of millions had been targeted," Sept. 25, 2003, http://www.msnbc.com/news/971869.asp?cp1=1; *see also* Audrey Hudson, "Data program must solve privacy fears, says the Pentagon," *Washington Times*, May 21, 2003, http://www.washingtontimes.com/national/20030521-125954-7816r.htm.

[120] "The Carnivore FOIA Litigation," http://www.epic.org/privacy/carnivore/; *see also* "Internet and Data Interception Capabilities Developed by the FBI," Statement for the Record of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, Before the United States House of Representatives, Committee on the Judiciary, Subcommittee on the Constitution, July 24, 2000, http://www.fbi.gov/congress/congress00/kerr072400.htm; "Carnivore Diagnostic Tool," Statement for the Record of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, Before the United States Senate, Committee on the Judiciary, Sept. 6, 2000, http://www.fbi.gov/congress/congress00/kerr090600.htm.

[121] "Answers to Frequently Asked Questions (FAQ) about Echelon," Feb. 7, 2002, http://archive.aclu.org/echelonwatch/faq.html.

[122] *Draft Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*, section "Motion for a Resolution," Temporary Committee on the ECHELON Interception System, European Parliament, 18 May 2001, http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf.

[123] *Id.*

[124] Jelle van Buuren, Hearing On Echelon In Dutch Parliament, Heise Telepolis, Jan. 23, 2001 (available at http://www.heise.de/tp/) and http://archive.aclu.org/echelonwatch/faq.html.

governments to conduct widespread surveillance on individuals and groups. Lack of anonymity, combined with "passive" monitoring techniques such as "cookies" and the more intrusive "clickstream" monitoring (a page-by-page tracking as a person wanders through the Internet) allows private sector entities to assemble detailed dossiers on individuals. This erosion of privacy is compounded by the weak privacy laws and regulations in the U.S., but is countered by the more stringent data protection afforded by the European Union.

A countervailing consideration is that the "anonymity enjoyed by today's cyber attackers poses a grave threat to the global information society, the progress of an information-based international economy, and the advancement of global collaboration and cooperation in all areas of human endeavor."[125] With respect to malicious cyber attacks by individual hackers and the more ominous case of attacks by nation states (including acts of cyber warfare),[126] the ability to deter attacks, obtain redress, or otherwise hold attackers accountable is directly linked to the ability to identify the sender and origin of the communication.[127] Therefore, it is imperative that interests in tracking and tracing be balanced with legitimate privacy interests and rights provided under international law.

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.

Much of the work in addressing developmental and digital divide issues is seen as falling within the purview of political and economic decisionmakers. However, the scientific community make significant contributions in this area because, among other reasons, of the rapid growth of peer-to-peer scientific networks which offer low-cost opportunities and solutions for developing countries.

ICTs bring both opportunities and challenges to developing countries.[128] The G8, World Bank, United Nations (UN), and U.S. Agency for International Development (USAID) are each committed to bridging the global "Digital Divide."[129] The donor community[130] also understands that ICTs are a powerful development tool that can help boost economies, increase competitiveness, attract foreign direct investment (FDI), and raise the skill level of the workforce in developing countries. Developing countries also realize the potential impact of technology, and many are launching their own ICT initiatives and aggressively competing for donor funds to assist them.

---

[125] Lipson at 4, http://www.cert.org/archive/pdf/02sr009.pdf.
[126] A discussion of cyber attacks from an arms control perspective is presented in V. Tsygichko, "Cyber Weapons as a New Means of Combat," http://www.itis-ev.de/infosecur
[127] Lipson at 18, http://www.cert.org/archive/pdf/02sr009.pdf.
[128] The explanatory comments for this Recommendation are, in large part, taken from the *International Guide to Combating Cybercrime*, which was written and copyrighted by Jody Westby. The *Cybercrime Guide* was written to assist developing countries understand cybercrime and the steps they needed to take to become active participants in combating cybercrime on a global scale. *See* Westby Cybercrime at 11-17, http://www.abanet.org/abapubs/books/cybercrime/.
[129] "Digital Divide" refers to "The gap between those able to benefit by digital technologies and those who are not." *See* http://www.digitaldivide.org.
[130] The donor community consists of aid institutions such as The World Bank Group, the U.S. Agency for International Development (USAID), United Nations (UN), Canada International Development Agency (CIDA), European bank of Reconstruction and Development (EBRD), Inter-American Development Bank (IADB), and numerous other development banks and assistance organizations.

Internet growth works in their favor. Today, there are approximately 600 million people connected to the Internet. However, that online population accounts for only 10% of a world population of about 6 billion people. Since 65% of Americans are already online,[131] we can expect some of the highest connectivity increases to be in the 180 developing countries around the globe. Indeed, Forrester Research predicts that by 2007, 70% of software programming will be performed in developing countries.[132]

Thus, developing countries have an unprecedented opportunity to seize upon the advantages of ICTs to propel their progression toward industrialization, market economies, and social advancements. These opportunities, many of which are directly dependent on inputs from the scientific community, include:

- Attracting foreign direct investment to (a) build infrastructure, (b) launch ICT projects, (c) partner with donor organizations and governments on pilot projects, and (d) tap undeveloped or under-developed markets.
- Privatizing and liberalizing monopoly providers to introduce competition, lower prices, and advance the deployment and utilization of ICTs.
- Attracting data processing applications such as data entry, customer service and telemarketing operations, records processing (accounts receivable, accounts payable, general ledger, etc.), order entry, inventory control, databank development, data storage operations, remote systems administration, etc.
- Attracting Internet start-up companies, e-commerce operations, and software development centers.
- Developing telemedicine and health care centers.
- Using ICTs for distance learning, education, brokerage services, and building workforce skills.
- Using ICTs for agri-business and agricultural information and industry sector support.
- Attracting light manufacturing operations.
- Modernizing the financial sector.
- Fostering the growth of small and medium-sized enterprises (SMEs) to spur job creation, innovation, flexibility, and competitiveness.
- Reforming and automating court administration and case management and availability of judicial information.

---

[131] Global Internet Statistics: Sources & References, Global Internet Statistics (by Language), Mar. 31, 2002, http://www.global-reach.biz/globstats/evol.html.
[132] "Taking up technology," *Financial Times*, Apr. 2, 2002, at 8.

While the contribution of the scientific community could be a force-multiplier, each of these opportunities, is largely dependent upon the development of the legal and regulatory framework to support these activities. The legal framework is one of the most important factors because it touches upon all aspects of commerce, is critical to attracting investment, and is at the core of providing certainty to business operations. The term "legal framework" also includes public policy, which forms the underlying foundation of government support for ICTs and a favorable business environment. Information and infrastructure security are two of the most important components.

With nearly 200 countries connected to the Internet, cybercrime has become a global issue that requires the full participation and cooperation of the public and private sectors in all countries, including the 180 developing countries around the globe. A major component of information and infrastructure security is a nation's ability to deter, detect, investigate, and prosecute cyber criminal activities. Weaknesses in any of these areas can compromise security not only in that country, but around the globe. This is due to the global, interconnected nature of the Internet and the way in which countries must rely upon each other's expertise and assistance in addressing cybercrime matters.

The confidentiality, integrity, and availability of data and networks – including critical infrastructure – are central to attracting FDI and ICT operations to developing countries. The opportunities associated with ICTs are not guaranteed; they are dependent upon developing countries' ability to effectively address the additional challenge of cyber security and to take steps to actively participate in the global community in combating cybercrime.

Appropriate security laws and regulations are also important because:

- They protect the integrity of the government and reputation of the country.
- They help preclude a country from becoming a haven for bad actors, such as terrorists, organized crime, and fraud operations.
- They help prevent a country from becoming a repository for cyber-criminal data.
- They instill market confidence and certainty regarding business operations and attract foreign direct investment.
- They provide protection of classified, secret, confidential and proprietary information, criminal justice data, personal information, and certain categories of public data.
- They protect consumers and assist law enforcement and intelligence gathering activities.
- They deter corruption.
- They increase national security and reduce vulnerabilities to attacks and actions by terrorists and other rogue actors.
- They help protect corporations against risk of loss of market share, shareholder and class action lawsuits, damage to reputation, fraud, and civil and criminal fines and penalties.
- They provide a means of prosecution and civil action for acts against information and infrastructure.

- They increase the chance that electronic evidence in physical-world crimes, such as murder or kidnapping, will be available when needed.

- They create an atmosphere of stability in which economic and social welfare can flourish.

For the most part, developing countries are struggling with how to use e-commerce and ICTs in everyday government and business operations.

The lack of an adequate legal framework – especially with respect to information and infrastructure security and computer crime – will diminish or prevent developing countries from grasping ICT opportunities. The reasons are clear:

- Internet and e-commerce operations require an enabling legal framework that also provides for security of data and networks.

- Data processing operations require information and infrastructure security laws for a safe operating environment and protection of data.

- Companies will not allow their data to be processed in countries that do not have adequate legal protections against economic espionage, computer crime, infrastructure attacks, and misuse of telecommunications devices and equipment.

- Certain laws, such as the EU data protection directive, require that countries afford equal legal protections against misuse of personal data.

Much of the inadequacies in addressing these critical issues in developing countries occur because of shortages in scientific and knowledge-based resources. Much is also due to scarcities in financial resources, which in turn constrict the enormous potential inherent in the large human resource base in the developing world. By helping identify and discover low-cost solutions, and by closer coordination with other relevant partners, the scientific community can unleash these human resources, and place them at the service of the developmental effort. The role of the World Federation of Scientists would be an important catalyst in this effort.

Deeper consideration of these issues is indicated in the future. The PMP intends to focus on some of these in subsequent meetings.

List of PMP Members

William A. Barletta
William A. Barletta is Director of the Accelerator and Fusion Research Division and the Office of Homeland Security at Lawrence Berkeley National Laboratory. He is an Editor of Nuclear Instruments and Methods A, an Editor of the Internet Journal of Medical Technology, Chairman of the Board of Governors of the U.S. Particle Accelerator School, and Member of the Governing Board of the Virtual National Laboratory for Heavy Ion Fusion. His recent research has concentrated on cyber security and the application of neutron sources and bright ion beams to nanotechnology and medicine.

Olivia A. Bosch
Olivia Bosch is currently a Senior Research Fellow in the New Security Issues Programme of The Royal Institute of International Affairs in London. Previously, she worked as a Senior Fellow at the Center for Global Security Research (Lawrence Livermore National Laboratory, Livermore, California) and at the International Institute for Strategic Studies in London.

Dmitry Chereshkin
Dr. Dmitry S. Cherechkin is an Academician and Vicepresident of the Russian Academy of Natural Sciences, where he is a Professor of Computer Sciences in the Institute for Systems Analysis. He currently acts as Deputy Chairman of the Government's Workshop Group to elaborate the Information Development Strategy of Russia.

Ahmad Kamal
Ambassador Ahmad Kamal served as a professional diplomat in the Ministry of Foreign Affairs of Pakistan for close to forty years until his retirement in 1999. During this period, he held diplomatic postings in India, Belgium, France, the Soviet Union, Saudia Arabia, the Republic of Korea, and with the United Nations both in Geneva and in New York. He continues to be a Senior Fellow of the United Nations Institute of Training and Research. He is also the Founding President and CEO of The Ambassador's Club at the United Nations.

Andrei V. Krutskikh
Prof. Dr. Andrei V. Krutskikh is a diplomat and politologist, specializing in issues of disarmament and international cooperation in the field of science and technology. He has served in diplomatic service in the Foreign Affairs Ministry (VFA) of Russia since 1973. He has been stationed at Russian embassies in the USA and Canada. Dr. Krutskikh was a member of the Russian negotiations teams for the SALT II and INF Treaties. At present, he serves as deputy director of the department in the MFA for security, technological, and disarmament affairs. He is a Member of the International Academies on Informatization and Telecommunication and a Professor at the Moscow State Institute/University on International Relations.

Axel H.R. Lehmann
Prof. Dr. Lehmann received his Studies of Electrical Engineering (Dipl.-Ing.) and received his doctorate of Informatics at the University of Karlsruhe in Germany. From 1982-1987, he was research assistant and Visiting Professor at the Universities of Karlsruhe and Hamburg. Since 1987,

Dr. Lehmann has been Full Professor for Informatics at the Faculty for Informatics, Universitaet der Bundeswehr Muenchen. Major positions and activities include Dean of the Faculty for Informatics (1995-1997) and member of the Academic Senat of the Universitaet. He served as Vice-President and President of the Society of Modeling and Simulation International from 1993-2000 and is a member of an Advisory Council for the Ministry of Science, Culture, and Research, Baden-Wuertternberg, Germany.

Timothy L. Thomas
Mr. Thomas works at the Foreign Military Studies Office at the U.S Army's Fort Leavenworth establishment in Fort Leavenworth, Kansas.

Vitali Tsygichko
Prof. Dr. Tsygichko is an expert of the Federal Assembly of the Russian Federation and professor at the Institute of Systems Analyses of the Russian Academy of Sciences. The author of six scientific books and more than 200 articles, Dr. Tsygichko is a Full Member of the Russian Academy of Natural Sciences and full professor of cybernetics in the field of system analyses and decision making systems for national security problems. He is a retired colonel and received his Doctor of Technical Sciences (Cybernetics) from Moscow University.

Henning Wegener
Dr. Henning Wegener serves as Chairman of the World Federation of Scientists Permanent Monitoring Panel on Information Security. A German diplomat and lawyer, Dr. Wegener, received his L.L.B. from the University of Bonn, his M.C.L. from George Washington University, and his LL.M. and J.S.D. from Yale University. He has undertaken further studies at the Sorbonne in Paris. Ambassador Wegener joined the German Federal Foreign Office in 1962. From 1981-1986 he was Ambassador in Geneva, from 1986-1991 he was Assistant Secretary General for Political Affairs of the North Atlantic Treaty Organization in Brussels. Dr. Wegener was Lecturer in Political Science at the Free University of Berlin from 1990-1995, and from 1991-1995 he was Deputy Secretary of the Federal Press and Information Office in Bonn. From 1995-1999 he was Ambassador of Germany to the Kingdom of Spain and to the Principality of Andorra. Since 2000, he has been a consultant in Madrid. He has published extensively on foreign and security policy.

Jody R. Westby
Ms. Westby is founder and President of The Work-IT Group, specializing in privacy and security, cybercrime, and information warfare. Previously, Ms. Westby was Chief Administrative Officer and Counsel of In-Q-Tel, Inc., a corporation devoted to finding unclassified, commercial solutions to IT problems facing the U.S. intelligence community. As a practicing attorney, Ms. Westby practiced international trade, technology, and intellectual property law with the New York firms of Paul, Weiss, Rifkind, Wharton & Garrison and Shearman & Sterling. As Senior Fellow and Director of Information Technology Studies for The Progress & Freedom Foundation, she directed and managed IT projects on an array of cutting-edge issues. Prior to that, Ms. Westby was Director of Domestic Policy for the U.S. Chamber of Commerce. Ms. Westby is chair of the American Bar Association's Privacy and Computer Crime Committee and was chair, co-author and editor of its *International Guide to Combating Cybercrime, International Strategy for Cyberspace Security,* and *International Corporate Privacy Handbook*.