THE QUEST FOR CYBER PEACE

International Telecommunication Union

THE QUEST FOR CYBER PEACE

By Dr Hamadoun I. Touré

Secretary-General of the International

Telecommunication Union

and

the Permanent Monitoring Panel on Information Security

World Federation of Scientists

January 2011

Legal notice

Authors individually retain copyright to their work. Third-party sources are quoted as appropriate. The International Telecommunication Union (ITU) is not responsible for the content of external sources including external websites referenced in this publication.

Neither ITU nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Disclaimer

The chapters in this publication represent the views of the individual authors, which are not endorsed by or intended to represent the views of any organization they may be employed by or affiliated with. Mention of and references to specific countries, companies, products, initiatives or guidelines do not in any way imply that they are endorsed or recommended by ITU, the authors, or any other organization that the authors are affiliated with, in preference to others of a similar nature that are not mentioned.

Acknowledgements

The ITU Secretary-General and the World Federation of Scientists would like to thank Jody Westby, Henning Wegener, and all the authors who have made it possible to put together their views on this emerging global concern. The Secretary-General also expresses gratitude to Prof. Antonino Zichichi, President of WFS, and his sincere thanks to the Head of the ITU Corporate Strategy Division, Alexander Ntoko, and especially JeoungHee Kim who led and coordinated this publication; to Rebekah Lewis, Deepti Venkateswar, Preetam Maloor, Marco Obiso and Elizabeth Aschenbrener; to Claude Briand and her team; and many others in ITU and WFS without whose contribution this publication would not have been possible

If you have any comments, please contact Corporate Strategy Division, International Telecommunication Union, at strategy@itu.int.

Copyright to Collective Work © 2011, International Telecommunication Union
& World Federation of Scientists

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

TABLE OF CONTENTS

Page

Table of Abbreviations iii

About the International Telecommunication Union and The Global Cybersecurity Agenda v

About the World Federation of Scientists and its Permanent Monitoring Panel on Information Security vi

Foreword (By Hamadoun I. Touré, Antonino Zichichi) xi

1 Introduction (By Jody R. Westby) 1

2 Cyberspace and the Threat of Cyberwar (By Hamadoun I. Touré) 7

3 Societal Dependencies and Trust (By Jacques Bus) 14

3.1 Modern Societies' Dependency on ICTs and the Internet 14

3.2 Socio-economic Implications of Cybercrime 26

4 Technology Trends and Threats 31

4.1 Current Potentials, Trends and Threats (By Axel Lehmann, Vladimir Britkov, Jacques Bus) 31

4.2 Government Internet Censorship: Cyber Repression (By Henning Wegener) 43

5 Cyber Conflict & Geo-Cyber Stability 53

5.1 Cyber Conflict (By Giancarlo A. Barletta, William A. Barletta, Vitali N. Tsygichko) 53

5.2 A Call for Geo-Cyber Stability (By Jody R. Westby) 66

6 Cyber Peace (By Henning Wegener) 77

A Concept of Cyber Peace 77

		Page
7	**The International Response to Cyberwar** (By Hamadoun I.Touré)	**86**
	7.1 National Policies and Approaches	*86*
	7.2 Recent International Responses	*91*
	7.3 Necessity of an International Framework	*96*
	7.4 Proposals for International Principles in Cyberspace	*100*
8	**ITU's Global Cybersecurity Agenda** (By Hamadoun I. Touré)	**104**
9	**Erice Declaration on Principles for Cyber Stability and Cyber Peace** (By World Federation of Scientists)	**110**
10	**Conclusion** (By Jody R. Westby)	**112**

Table of Abbreviations

AIS	Automated Information Systems
ARPA	Advanced Research Projects Agency (U.S. Department of Defense)
C3	Command, Control & Communications
CoE	Council of Europe
COP	Child Online Protection Initiative (ITU)
CRS	Congressional Research Service (U.S.)
CSCW	Computer Supported Cooperative Work
DARPA	Defense Advanced Research Projects Agency (U.S. Department of Defense)
DNS	Domain Name System
ECOSOC	Economic and Social Council (UN)
ESCAPE	Electronically Secure Collaboration Application Platform for Experts (IMPACT)
EU	European Union
FG Smart	Smart Grid Focus Group
FTC	Federal Trade Commission (U.S.)
GCA	Global Cybersecurity Agenda (ITU)
GRC	Global Response Center (IMPACT)
HRC	Human Rights Committee (HRC)
ICT	Information and Communication Technology
IGF	Internet Governance Forum
IMPACT	International Multilateral Partnership Against Cyber Threats (Malaysia)
IP	Internet Protocol
ISOC	Internet Society
IT	Information Technology
ITR	International Telecommunication Regulations (ITU)
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LOAC	Laws of Armed Conflict
MIT	Massachusetts Institute of Technology
NATO	North Atlantic Treaty Organization
NEWS	Network Early Warning System (IMPACT)
NPT	Non-Proliferation of Nuclear Weapons Treaty
NSF	National Science Foundation

RFID	Radio-Frequency Identification
PDA	Personal Digital Assistant
PMP	Permanent Monitoring Panel of Information Security (WFS)
SCADA	Supervisory Control and Data Acquisition
SOA	Service Oriented Architectures
TCP	Transmission Control Protocol
UN	United Nations
UNCPCJ	United Nations Congress on Crime Prevention and Criminal Justice (UN)
UNESCO	United Nations Educational, Scientific, and Cultural Organization (UN)
UNODC	United Nations Office of Drugs and Crime (UN)
URL	Uniform Record Locator
WFS	World Federation of Scientists
WSIS	World Summit on the Information Society

About the International Telecommunication Union and The Global Cybersecurity Agenda

The International Telecommunication Union (ITU) is the leading United Nations agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services.

A fundamental role of ITU following the World Summit on the Information Society (WSIS) and the 2006 ITU Plenipotentiary Conference is to build confidence and security in the use of information and communication technologies (ICTs). Heads of States and government and other global leaders participating in WSIS, as well as ITU Member States, entrusted ITU to take concrete steps towards curbing the threats and insecurities related to the information society. To fulfill this mandate, ITU Secretary-General Dr Hamadoun I. Touré launched the Global Cybersecurity Agenda (GCA) as a framework for international cooperation in 2007.

The GCA aims to enhance confidence and security in the information society. It is designed for cooperation and efficiency, encouraging collaboration between all relevant stakeholders and building on existing initiatives to avoid duplicating efforts. The GCA is the first truly global multistakeholder and public–private alliance against cyberthreats. In 2008, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) formally entered into a Memorandum of Understanding, after which IMPACT's state-of-the-art headquarters in Cyberjaya, Malaysia, became the physical home of the GCA. IMPACT is an international public–private initiative dedicated to enhancing the global community's capacity to prevent, defend and respond to cyberthreats. This collaboration provides ITU's 192 Member States and others with the expertise, facilities and resources to effectively enhance the global community's capability and capacity to prevent, defend against and respond to cyberthreats. Since its launch, the GCA has attracted the support and recognition of leaders and cybersecurity experts around the world. H.E. Dr. Óscar Arias Sánchez, former President of the Republic of Costa Rica and Nobel Peace Laureate, and H.E. Blaise Compaoré, President of Burkina Faso, are both Patrons of the GCA.

The GCA has fostered initiatives such as Child Online Protection (COP), the Cybersecurity Gateway and, through its partnership with IMPACT and with the support of leading global players, is currently deploying cybersecurity solutions to countries around the world. ITU would like to thank H.E. Laura Chinchilla, President of Costa Rica in her role as Patron of ITU's COP.

About the World Federation of Scientists and its Permanent Monitoring Panel on Information Security

The World Federation of Scientists (WFS) was founded in Erice, Sicily, in 1973, by a group of eminent scientists led by Isidor Isaac Rabi and Antonino Zichichi. Since then, many other scientists have affiliated themselves with the Federation, among them T. D. Lee, Laura Fermi, Eugene Wigner, Paul Dirac and Piotr Kapitza.

The WFS is a free association, which has grown to include more than 10,000 scientists drawn from 110 countries**.** All members share the same aims and ideals and contribute voluntarily to uphold the Federation's Principles. The Federation promotes international collaboration in science and technology between scientists and researchers from all parts of the world – North, South, East and West. The Federation and its members strive towards an ideal of free exchange of information, where scientific discoveries and advances are no longer restricted to a select few. The aim is to share this knowledge among the people of all nations, so that everyone may experience the benefits of the progress of science.

The creation of the World Federation of Scientists was made possible by the existence, in Erice, of a centre for scientific culture named after the physicist Ettore Majorana, the ***Ettore Majorana Foundation and Centre for Scientific Culture*** (Centre). This Centre, which has been dubbed "The University of the Third Millennium," has become a global educational force. Since its founding in 1963, the Centre has conducted 123 schools and 1,497 courses for 103,484 participants (125 of which are Nobel Laureates), coming from 932 universities and laboratories of 140 nations.

The Ettore Majorana Centre was a precursor of the World Federation of Scientists and its action to mitigate planetary emergencies. The World Federation of Scientists rapidly identified 15 classes of **Planetary Emergencies** and began to organize the fight against these threats. One of its main achievements was the drawing up of the **Erice Statement**, in 1982, by Paul Dirac, Piotr Kapitza and Antonino Zichichi, clearly setting out the ideals of the Federation and putting forward a set of proposals for putting these ideals into practice. Another milestone was the holding of a series of International Seminars on Nuclear War which have had a tremendous impact on reducing the danger of a planet-wide nuclear disaster and have ultimately contributed to the end of the Cold War. In 1986, through the action of a group of eminent scientists (most of whom were members of the WFS) the International Centre for Scientific Culture **ICSC-World Laboratory** was founded in Geneva to help achieve the goals outlined in the Erice Statement.

WFS established its Permanent Monitoring Panel (PMP) on Information Security in 2001. Its report, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar,* was one of the leading documents filed by the civil society in the United Nations' World Summit on the Information Society (WSIS) first held in Geneva in 2003. The PMP has published numerous papers on cybersecurity and cyberwarfare and regularly presents information security issues as a critical planetary emergency topic in WFS plenary sessions held each August in Erice. In August 2009, the PMP was so alarmed by the potential of cyberwarfare to disrupt society and cause unnecessary harm and suffering, that it drafted the **Erice Declaration on Principles of Cyber Stability and Cyber Peace**, which was adopted by the Plenary of the WFS on the occasion of the 42nd Session of the International Seminars on Planetary Emergencies in Erice on 20 August 2009. The Declaration has been distributed to every Member States of the United Nations.

The PMP is co-chaired by Amb. Henning Wegener of Berlin & Madrid and Dr Jody R. Westby, CEO of Global Cyber Risk LLC, in Washington, DC. Its members contributing to this publication include:

CONTRIBUTING PMP MEMBERS

William Barletta

William A. Barletta is the Executive Director of the United States Particle Accelerator School, a national graduate program. He is Adjunct Professor of Physics at the Massachusetts Institute of Technology and at the University of California Los Angeles. He is also Visiting Full Professor of Economics at the University of Ljubljana, Slovenia, where he teaches strategic management, and senior advisor to the President of Sincrotrone Trieste, Italy. He is a Fellow of the American Physical Society, a member of its Panel on Public Affairs, vice-chair of its Forum on International Physics and vice-chair of its Division of Physics of Beams. He is co-author and editor of five books and the author of more than 150 articles covering a very wide range of technological topics. barletta@mit.edu

Vladimir Britkov

Vladimir B. Britkov (Ph.D.) is the Head of the Information Modeling Laboratory in the Institute for Systems Analysis of the Russian Academy of Sciences, Moscow, Russia. He is an Adjunct Professor of Systems Analysis and Systems Modeling in the Moscow Institute of Physics and Technologies (State University). His major areas of research include computer-based modeling and simulation and application of knowledge-based

systems for decision support. He has served as a member of the Board of the Directors of The International Emergency Management Society (TIEMS). He is a member of various editorial boards of scientific journals in the fields of modeling and simulation, and of various international working groups. He has been a member of the World Federation of Scientists Permanent Monitoring Panel on Information Security since 2003. britkov@gmail.com

Jacques Bus

Jacques Bus is an independent consultant at *Digitrust.EU* working in the area of Trust and Security in Information and Communication Technology (ICT) and a Research Fellow at the University of Luxembourg. After 12 years of research in Mathematics he focused on research management and worked for more than 20 years in the ICT Research Programme of the European Union, the last six years of which he worked as Head of Unit *ICT Trust and Security*. He is a member of the World Federation of Scientists Permanent Monitoring Panel on Information Security. He publishes and speaks on issues of trust, security, privacy and identity management. www.digitrust.eu

Axel Lehmann

Axel Lehmann is Full Professor at the Department for Informatics at the Universität der Bundeswehr München where he holds a chair for modeling and simulation. He is also chairman of the university's Institute for Intelligent Systems (ITIS). His major areas of research range from computer-based modeling and simulation, application of knowledge-based systems for diagnosis and decision support, to design of innovative computer architectures. He is a former president of the Society for Modeling and Simulation International, a Fellow of the German Informatics Society, a member of various editorial boards of scientific journals in the fields of modeling and simulation, and a member of international working groups and evaluation committees, e.g. for the European Union. He has been a member of the WFS PMP since 2001.
axel.lehmann@unibw.de

Hamadoun I. Touré

Dr Hamadoun I. Touré, Secretary-General of the International Telecommunication Union (ITU) since January 2007, was re-elected for a second term at the ITU Plenipotentiary Conference, Guadalajara, Mexico, in October 2010. He served as Director of ITU's Telecommunication Development Bureau (BDT) from 1998 to 2006, and has wide professional experience in both the public and private sectors. Born in 1953, Dr Touré holds a Masters Degree in Electrical Engineering from the Technical Institute of Electronics and Telecommunications of Leningrad (LEIS, USSR) and Doctor

of Philosophy Degree (PhD) from the University of Electronics, Telecommunications and Informatics of Moscow (MTUCI, Russia). He is committed to ITU as an innovative, forward-looking organization adapted to meeting the challenges created by the rapidly changing ICT environment, and to continuing to spearhead the Union towards implementing the resolutions of the World Summit on the Information Society (WSIS) and achieving the Millennium Development Goals (MDGs). hamadoun.toure@itu.int

Vitali Tsygichko

Dr V.N. Tsygichko, Colonel, Russian Army, Ret., is a full member of the Russian Academy of Natural Sciences, and since 1985 the chief researcher at the Institute of Systems Analysis of the Russian Academy of Sciences (ISA RAS). He is currently the Russian Federation's Ministry of Foreign Affairs expert on information security problems. Since 1967 he has served the Central Research Institute of the Ministry of Defense, working on mathematical simulations of military operations. From 1988-1991 he headed an autonomous Center for Research into National Security Problems. Dr Tsygichko's range of scientific interests embraces methodological and systematic problems of modeling socio-economic processes; decision theory; applied systems analysis; the theory and methods of socio-economic forecasting; ensuring national security and strategic stability; information security problems; and geopolitical problems. He has authored over 200 papers and eight books. He is a permanent author of journals such as Military Thought, Military Bulletin, Independent Military Review, and a number of foreign publications. He is a graduate of the Ryazan Artillery Military School, the Dzerzhinsky Military Academy, and holds a Doctor of Science (Engineering) and Professor. vtsygichko@inbox.ru

Henning Wegener

Henning Wegener is a former Ambassador of Germany. He served as Ambassador for Disarmament in Geneva (1981–1986), Assistant Secretary-General for Political Affairs at NATO (1986–1991) and later as Ambassador to Spain. Ambassador Wegener was Chairman (2001–2009) and is now Co-Chair of the World Federation of Scientists Permanent Monitoring Panel on Information Security. His work has been featured in publications in the field of foreign and security policy, including cybersecurity. Among other degrees Mr Wegener holds a Doctor of Juridical Science from Yale Law School. henningwegener@hotmail.com

Jody R. Westby

Jody R. Westby is CEO of Global Cyber Risk LLC, based in Washington, DC, and also serves as Adjunct Distinguished Fellow to the Carnegie Mellon CyLab. Ms Westby

provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, cybercrime, critical infrastructure protection, and economic espionage. She is chair of the American Bar Association's (ABA) Privacy & Computer Crime Committee (Section of Science & Technology Law) and represents the ABA on the National Conference of Lawyers and Scientists. Ms Westby was a member of the ITU Secretary-General's High-Level Experts Group and led the development of the *ITU Toolkit for Cybercrime Legislation*. She co-chairs the World Federation of Scientists Permanent Monitoring Panel on Information Security. Ms Westby is co-author and editor of four books on international cybercrime, cybersecurity, and privacy and has published numerous articles. She speaks globally on these topics. westby@globalcyberrisk.com

Foreword

In the world of 2011, we enjoy the benefits of a boundless global information society, but with these benefits comes the threat of cyber attacks. They can arise anywhere, at anytime, and cause immense damage in the blink of an eye. This potential damage is increased exponentially by the linking of information and communication technologies (ICTs) with vital national infrastructures.

We must act now to stem this growing threat.

At the World Summit on the Information Society (WSIS), world leaders and governments entrusted the International Telecommunication Union (ITU) with the task of coordinating a mechanism for building confidence and security in the use of ICTs. Since that time, Secretary General Touré has launched the Global Cybersecurity Agenda (GCA), and ITU has actively pursued fulfillment of this mandate through a number of initiatives. Above all else, ITU remains deeply concerned about cyberthreats among its Member States.

The World Federation of Scientists (WFS) promotes international collaboration in science and technology between scientists and researchers from all parts of the world. It strives to advance the free exchange of information so that everyone can benefit from the progress of science. In 2009, the WFS's Permanent Monitoring Panel (PMP) on Information Security drafted the Erice Declaration on Principles of Cyber Stability and Cyber Peace, which calls for concerted, international action to ensure that information networks and systems remain stable, reliable, available, and trusted. The Declaration was adopted by the Plenary of the WFS on the occasion of the 42nd Session of the International Seminars on Planetary Emergencies in Erice (Sicily) on 20 August 2009 and has been distributed to every Member State of the ITU.

To achieve the mutual goal of ensuring Cyber Peace, collaboration between ITU and members of the science and technology community is critical. We cannot effectively confront the threat of cyberwar without the involvement of those with expert knowledge and insight of the technologies that are changing the global landscape.

This volume gives voice to that community. It represents a necessary step in the process of building international cooperation to address these challenges. We are grateful for the opportunity to present all our views on this critical issue.

Dr Hamadoun I. Touré
Secretary-General
International Telecommunication Union

Professor Dr Antonino Zichichi
President
World Federation of Scientists

1 Introduction

By Jody R. Westby

This publication aims to promote the concept of global cyber peace by:

- Examining how ICTs underpin everyday life;
- Evaluating current cyberthreats and trends;
- Analysing the impacts of cybercrime and cyber conflict;
- Assessing the validity of current legal frameworks;
- Defining the concept of cyber peace, and establishing it as an overriding guiding principle for peaceful behaviour in cyberspace; and
- Charting a path forward.

The Internet is the central nervous system of society. Consider that every critical infrastructure sector is dependent upon ICTs. They are controlled by supervisory control and data acquisition (SCADA) systems and other complex information technology (IT) processes that are connected in some fashion to the Internet. For example, hospitals and medical centers utilize ICTs for everything from emergency dispatch to life support systems. The oil and gas and transportation sectors deploy sophisticated processing and navigational systems that are fully computerized, and financial companies operate through e-payment systems and electronic processing. Governments are dependent upon ICTs to deliver services, manage operations across diverse geographical areas, maintain public safety and protect their territories. Businesses rely upon computer systems that manage supply chains, customer relations, financial flows, and perform manufacturing functions. And the communication systems and utility grids are the "super critical" infrastructures upon which all others are dependent.

The Internet also is now integrally woven into the everyday functions and lives of the individual. Whether working, learning or playing, ICTs play a role. The Internet enables the propagation of knowledge and information at a level unprecedented in world history. The power of social networking links populations and influences them in ways completely separate from, or unanticipated by, their governments. It has enabled the empowerment of the individual, the expansion of the self, and the dissemination of uncommon ideas via a mechanism that is largely blind to borders and diplomatic or political considerations. Today, an individual can rapidly impact perceptions, values, ideas, and biases simply through their ability to create content and distribute it globally.

The pervasiveness of the Internet, however, also has spawned criminal activities and created new avenues for intelligence gathering and conflict. Vulnerabilities within operating systems, software, and security settings enable exploits that threaten basic services to civilian populations, facilitate economic espionage, and impact government operations. Viruses, worms, distributed denial of service (DDoS) attacks, theft of proprietary data, spam, and fraud all undermine the reliability of ICTs and the ability of societies and economies to function.

Effective security programs will improve the resilience of systems and help detect, prevent, and mitigate such actions. Technological patches and new innovations will help block and track attacks, and harmonized cybercrime laws will advance the investigation and prosecution of cybercriminals. There is much work to be done in each of these areas, but the most dangerous and potentially destructive problem is when nation states employ such tactics to wage cyber conflict.[1] There are now numerous examples of how political and military conflicts spill over into cyberspace, effectively undermining trust in ICTs and presenting serious risks. Several of these instances are described in the subsequent chapters of this publication.

Before the advent of the information society, power and leadership were usually held by those with political authority, military superiority, and economic dominance. Nation States and international organizations dictated social norms and values, and armed conflict was governed by laws and treaties based around territorial integrity and defensive capabilities in land, air, and sea. Today, however, the Internet has drastically shifted this balance of power. Nothing illustrates this point better than the history of the Internet itself.

World events can be important motivators. On the heels of World War II, America was faced with a new kind of enemy: the Cold War, communism, and threats of nuclear strikes. In response to concerns about Soviet scientific supremacy after their launch of the Sputnik, the first artificial earth satellite, President Eisenhower founded the U.S. Defense Department's Advanced Research Projects Agency (ARPA), now DARPA, to coordinate all U.S. technological research.[2] J.C.R. Licklider was hired from the Massachusetts Institute of Technology (MIT) to head up ARPA's computer research

---

1 The term cyber conflict is intended to include scenarios that may be labeled as "cyberwarfare."

2 "A Brief History of the Net," *Fortune*, 9 Oct. 2000 at 34, http://money.cnn.com/magazines/fortune/fortune_archive/2000/10/09/289297/index.htm (hereinafter "Fortune"); *see also* Dave Krisula, "The History of the Internet," Aug. 2001 (expanded 2009), www.davesite.com/webstation/net-history1.shtml (hereinafter "Krisula").

program. A few months before, he had published a series of memos discussing a "Galactic Network" of interconnected computers that enabled shared access to programs and files. Vint Cerf, Bob Kahn, and some of the other "Fathers of the Internet" later noted that, "In spirit, the concept was very much like the Internet of today."[3]

About that same time, the Air Force, concerned about its ability to maintain command and control operations following a nuclear attack, commissioned RAND to do a study on a survivable military network that could provide "minimum essential communications."[4] The RAND work (1962–1965) concluded with a report by Paul Baran describing how a packet switched computer network could provide this capability.[5] Simultaneously (and unbeknownst to the RAND group), three MIT engineers were discussing the concept of networked computers and packet switching.[6] In late 1966, one of the MIT engineers, Lawrence Roberts, moved over to DARPA "to develop the computer network concept".[7]

The rest is well known history. In 1971, the ARPANET, as the Internet was first called, had 23 hosts connecting government research centers and universities across the United States. By 1981, it was called the Internet, and by 1991, the World Wide Web, developed at the European Organization for Nuclear Research (also known as CERN), by Sir Timothy Berners-Lee,[8] came into existence. The combination of the Internet and Web ignited ideas of commercial use, but corporations were blocked from accessing the backbone through the National Science Foundation's (NSF) NSFNET.

---

3 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet," Internet Society (ISOC) All About the Internet, www.isoc.org/internet/history/brief.shtml (hereinafter "A Brief History of the Internet"); Licklider published his series of "Galactic Network" memos in August 1962 and began at ARPA in October 1962.

4 Krisula; see *also* Fortune; Stewart Brand, "Founding Father," *Wired*, Mar. 2001 at 148, www.wired.com/wired/archive/9.03/baran_pr.html (hereinafter "Brand").

5 Brand at 145-153; *see also* Krisula.

6 A Brief History of the Internet; *see also* Brand at 146; Krisula.

7 A Brief History of the Internet.

8 Elizabeth D. Hoover, "The Inventor of the World Wide Web," *AmericanHeritage.com,* 12 Nov. 2005, www.americanheritage.com/articles/web/20051112-internet-world-wide-web-tim-berners-lee-computer-geneva-cern-enquire-html-url-world-wide-web-consortium.shtml.

In 1995, the NSF acquiesced and turned access to the Internet backbone over to four commercial companies, and, by 1996, there were nearly 10 million hosts online and the Internet spanned the globe. Within three decades, the Internet grew "from a Cold War concept for controlling the tattered remains of a post-nuclear society to the Information Superhighway."[9] The combined Internet and World Wide Web has permeated economies and societies at all its layers and created social transformation that was unthinkable 20 years ago. Today, there are nearly two billion online users, and there are no geographical boundaries on the Internet. Management of the Internet today encompasses both technical and public policy issues and involves all stakeholders and relevant intergovernmental and international organizations.

The irony is that this brainchild of the Cold War era, combined with the internationalization in science that led to the Web, now presents one of the most critical challenges to global peace. Although geo-political[10] factors still must be accorded great weight in analysing national and economic security interests, the Internet has changed traditional analysis of foreign policy. Geo-cyber dimensions increasingly impact the conduct of nation states and geo-political blocks are forcing a new paradigm to emerge.

It is no longer a question of the U.S. maintaining "essential minimum communications": it is a question of how *all* countries around the world can maintain geo-cyber stability and ensure their critical infrastructures cannot be used as a weapon against innocent and defenceless civilians, resulting in unnecessary suffering and destruction.

The author defines "geo-cyber" as the relationship between the Internet and the geography, demography, economy, and politics of a nation and its foreign policy. "Geo-cyber stability" is defined as the ability of all countries to utilize the Internet for

---

9 "Life on the Internet: Net Timeline," PBS, www.pbs.org/opb/nerds2.0.1/timeline/; *see also* Krisula.

10 Geopolitics is defined as "(1) The study of the relationship among politics and geography, demography, and economics, especially with respect to the foreign policy of a nation, (2) a. A governmental policy employing geopolitics. b. A Nazi doctrine holding that the geographic, economic, and political needs of Germany justified its invasion and seizure of other lands, (3) A combination of geographic and political factors relating to or influencing a nation or region." American Heritage Dictionary, 2000, www.dictionary.com/search?q=geo-political.

economic, political, and demographic benefit while refraining from activities that could cause unnecessary suffering and destruction.[11]

Today, the entire world faces new threats arising from the Internet, and the ability of every nation state to maintain its communications, command, control and computer (C4) capabilities against attacks from terrorists, organized criminal rings and other nation states has become uncertain. ICTs present countries with unprecedented challenges to national and economic security. Individuals can now thwart authority and conduct asymmetrical attacks that can paralyze an entire infrastructure and stall communications, and the weakest systems can now threaten the security of the greatest of nations.

Cyber conflict can have life-threatening consequences when critical information infrastructures are impaired. It also can lead to information operations that impinge on international human rights, provoke violence and cause grave economic damage. The risks to individuals and nation states are enormous – and untethered from current legal frameworks that do not adequately accommodate the cyber age.

The need is urgent. The rapid pace at which countries are standing up cyber commands and expanding their military capabilities to include cyber conflict must be balanced by an agreement among nation states that recognizes a new level of "essential minimum communications" that are protected from conflict. Such action will prevent unnecessary destruction and suffering between those involved in a conflict, and it will protect other uninvolved countries from harm. Such a level of geo-cyber stability is vital, lest the benefits of the Internet be lost to the destructive forces of technology.

Multinational organizations are the logical starting point. They must begin by defining the minimum level of infrastructure and communication stability needed to protect innocent civilians and preserve basic societal functions, and ensure this through diplomatic agreement and the rule of law. This will require input from a wide array of stakeholders, including individuals, industry, civil society, academia, attorneys, policy experts, first responders, and law enforcement. In this manner, ICTs and the Internet can provide a positive international framework for collaboration between countries and lead to a better understanding and acceptance of differing cultural and societal values worldwide.

---

11 First presented at the ANSER Institute of Homeland Security Conference, "Homeland Security 2005: Charting the Path Ahead," University of Maryland, Presentation by Jody Westby, " A Shift in Geo-Cyber Stability and Security," 6–7 May 2002.

This book is predicated on the concept of cyber peace as the orienting principle for behaviour in cyberspace. Cyber peace should, therefore, be the quest of all nations. The advantages of cyber peace far outweigh the destructive consequences of cyber conflict.

This publication, co-authored by Hamadoun I. Touré, Secretary-General of the International Telecommunication Union, and members of the World Federation of Scientists Permanent Monitoring Panel on Information Security, is intended to serve as a call to action by all stakeholders to engage in efforts to ensure a minimum level of stability in the Internet and their infrastructures and advance the concept of global cyber peace.

2 Cyberspace and the Threat of Cyberwar

By Hamadoun I. Touré

Information and communication technologies (ICTs) have become an integral part of everyday life for many people of the world. Digital communications, networks and systems provide vital resources and indispensable infrastructure throughout the global community, necessities without which many populations could not flourish or even survive. These structures and systems represent a new domain, and with it come new challenges for preserving peace and stability. Without mechanisms for ensuring peace, cities and communities of the world will be susceptible to attacks of an unprecedented and limitless variety. Such an attack could come without warning. Suddenly, computers and cell phones will cease to function, cash-dispensing and banking machine screens will stare blankly at customers, air traffic control, railroad and motor traffic systems will leave highways, bridges and waterways in chaos and perishable goods stranded far from hungry populations. With the loss of electricity, hospitals, houses, shopping centres, whole communities will tumble into darkness. Government authorities will be unable to take stock of the damage, communicate with the rest of the world to spread word of the crisis or protect their vulnerable citizenry from subsequent attacks. This is the intractable plight of a community paralysed by the instantaneous loss of digital networks. This is the potential devastation of a new kind of war, a "Cyberwar."

A New Domain: Cyberspace, Security and Warfare

The threat of cyberwar now looms larger than ever. Today, technological advancements and growing digital infrastructure bind whole populations to complex, intertwined systems. Demand for Internet and digital connectivity calls for an ever increasing integration of ICTs into products that previously functioned without it, such as cars, buildings and even control systems for vast power and transportation grids. Electricity supply, transportation systems, military services and logistics – virtually all modern services depend on the use of ICTs and the stability of cyberspace. "Cyberspace" is the physical and conceptual realm in which all these systems exist. Therefore, "cyberwar" may be broadly understood as a war fought in cyberspace using

and targeting ICTs.[12] Rapidly increasing dependence on smart grids and other Internet-based control and monitoring systems places the heart of energy, transportation and defence resources within reach of those who seek to wreak havoc on government and civilian populations.[13] Thus, enhancing cybersecurity and protecting critical information infrastructures are now essential elements of each nation's security and economic well-being.

As global reliance on ICTs has grown, so has vulnerability to attacks on critical infrastructures through cyberspace. Although the exact contours of a "cyberwar" are still undefined, substantial attacks against information infrastructure and Internet services in the last decade provide some sense of the potential shape and scope of a conflict in cyberspace. Attacks in Georgia,[14] Estonia,[15] South Korea and the United States[16] have been linked with cyberwarfare. Multiple blackouts in Brazil have been connected to cyber attacks and, in 2008, hackers broke into the Government's website and took control of it for over a week.[17] The blackouts in Brazil illustrate the possible breadth of emerging kinds of cyber attacks: reports liken the scene to a science fiction film, with subway trains, traffic lights and the world's second largest hydroelectric

---

12 Steven Elliot, "Analysis on Defense and Cyberwarfare," *Infosec Island*, 8 July 2010, https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html (hereinafter "Elliot").

13 Ellen Messmer, "Cyberattack Seen as Top Threat to Zap U.S. Power Grid," *NetworkWorld*, 2 June 2010, www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html (reporting that the threat of a coordinated cyber attack, which might be combined with a physical attack, is considered the most pressing "high-impact, low-frequency" threat to North American electricity supply) (hereinafter "Messmer").

14 Thomas Claburn, "Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google And Elsewhere," *InformationWeek*, 12 Aug. 2008, www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702.

15 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 Aug. 2007, www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

16 Choe Sang-Hun and John Markoff, "Cyber attacks Jam Government and Commercial Web Sites in U.S. and South Korea," *The New York Times*, 8 July 2009, www.nytimes.com/2009/07/09/technology/09cyber.html; Jack Date, Jason Ryan, Richard Sergay, and Theresa Cook, "Hackers Launch Cyberattack on Federal Labs," *ABC News*, 7 Dec. 2007, http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1.

17 Michael Mylrea. "Brazil's Next Battlefield: Cyberspace," *Foreign Policy Journal*, 15 Nov. 2009, http://foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace (hereinafter "Mylrea").

power producer, the *Itaipu* dam, brought to a crashing halt and more than 60 million people affected.[18]

Cyberwar might also involve the private sector. Web service giants like *Google*[19] and *Twitter*[20] already experienced attacks in 2009 and, as early as 2000, denial-of-service attacks were launched against well known companies such as *CNN, Ebay* and *Amazon*.[21] As a result, some of the services were not available for several hours or even days. Hackers have targeted airport control systems, disabling critical equipment like phone services and runway lights.[22] By some counts, more than six countries have experienced cyber assaults in the past three years and at least 34 private companies were attacked in the early months of 2010 alone.[23] Though these security concerns are serious, it is not too late to stave off potentially catastrophic scenarios by creating safer products, practices and standards through a collaborative international effort.[24] Making the Internet safer and protecting ICTs from disruption and destruction must be priorities if we are to protect civilian populations, ensure the effective functioning of basic structures and provide for the continued development of new services.

Cyberwar as a Threat to National Infrastructure

The concept of cyberwar encompasses the targeting of not only military capabilities and systems, but also a society's vital infrastructure – including Smart Grids and supervisory control and data acquisition (SCADA) networks – that allows it to function and defend itself. While using a different medium (cyberspace and the ICTs operating

---

18 *Id*.

19 Andrew Jacobs and Miguel Helft, "Google, Citing Attack, Threatens to Exit China," *The New York Times*, Jan. 12, 2010, www.nytimes.com/2010/01/13/world/asia/13beijing.html.

20 Eliot Van Buskirk. "Denial-of-Service Attack Knocks Twitter Offline (Updated)," Wired.com, 6 Aug. 2009, www.wired.com/epicenter/2009/08/twitter-apparently-down/.

21 *See* Abraham D. Sofaer and Seymour E. Goodman, *The Transnational Dimension of Cyber Crime and Terrorism,* 2001 at 14, http://media.hoover.org/documents/0817999825_1.pdf.

22 *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, United States Government Accountability Office, Sept. 2007, GAO-07-1036, www.gao.gov/new.items/d071036.pdf. In 1997 (hackers attacked the Worcester Airport in the U.S., disabling phone services to the airport tower and shutting down the control system managing the runway lights).

23 Elliot.

24 Joshua Pennell, "Securing the Smart Grid: The Road Ahead," at 2, *NetworkSecurityEdge.com*, 5 Feb. 2010, www.networksecurityedge.com/content/securing-smart-grid-road-ahead.

in it), opponents can still deploy weapons and engage in an offensive–defensive conflict much like traditional warfare. Cyberwarfare tactics typically involve data collection or infiltration of computerized systems to cause damage to critical systems.[25] Potential cyber weapons include: computer viruses and worms, cyberdata collection exploits, wireless data communications jammers, compromised counterfeit computer software, electromagnetic pulse weapons, computer and networks reconnaissance tools and embedded Trojan time bombs.

Increasing reliance on smart grids leaves many countries' power supplies particularly vulnerable to attack. Smart grids are digitized systems which connect utility supplies to a central monitoring network, often called a SCADA network. SCADA networks gather information about power use and supply, while smart grids provide a digitized channel for that information to flow between consumers and suppliers.[26] These technologies are now used for a wide variety of processes and systems, including: water management systems, gas pipelines, electrical power transmission and distribution, wind power systems, mass communication systems, manufacturing, production, mass transit systems, environmental control systems, air traffic control and traffic lights.[27] More and more, suppliers are connecting smart grids to the Internet in order to allow for remote access and increased functionality.

While connected grids offer substantial benefits, such as reduction of energy waste and faster communication between customers and providers, they also centralize data and control of huge power grids on a network that has multiple access points. With more endpoints and more interconnected networks, smart grids and SCADA networks provide numerous ways for attackers to infiltrate them.[28] For example, a smart meter (an electrical meter connected to the grid) can be hacked and infected fairly easily, and it can then be used to spread a worm to other meters and eventually cause the power grid to surge or shut off.[29] Though many firms seek to secure their grids by

---

25 Elliot.

26 "Smart Grid," U.S. Department of Energy, www.oe.energy.gov/smartgrid.htm; "SCADA," *TopBits.com*, www.tech-faq.com/scada.html (hereinafter "SCADA").

27 SCADA.

28 Katie Fehrenbacher, "10 Things to Know About Smart Grid Security," 9 Oct. 2009, Earth2Tech, Gigaom, http://gigaom.com/cleantech/10-things-to-know-about-smart-grid-security/, (hereinafter "Fehrenbacher"}.

29 *Id*.

isolating control centres from other networks (a technique called "air-gapping"), these attempts to completely seal off certain components often fail, often unbeknownst to the administrator of the system.[30] Logic bombs are another way attackers might disrupt or even destroy a smart grid; hackers might infiltrate the grid to hide malicious software in it, waiting to activate these bombs at a later time for a coordinated assault or to cause limited power failures.[31] Such bombs create an additional security problem because they could be detonated accidentally or by a different hacker who discovers them at a later date.[32]

Already, countries that have invested in smart grids are reporting attempted attacks and probes numbering in the thousands per day.[33] By some estimations, cyber attacks are the greatest threat to national power-generation grids.[34] A remote attack could very well target physical infrastructure like power generators and transformers, causing them, in essence, to self-destruct.[35] Such an attack would most likely have long-range consequences, as power companies do not usually store expensive replacement parts, which can take months to manufacture and deliver.[36] An attack on a smart grid would not only leave customers without power, but it would also create massive financial damage. Power generators can run in the multi-million dollar range

---

30 "SCADA Security and Terrorism: We're Not Crying Wolf," at 26, BlackHat, www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

31 Siobhan Gorman. "Electricity Grid in U.S. Penetrated By Spies," *The Wall Street Journal,* 8 Apr. 2009, http://online.wsj.com/article/NA_WSJ_PUB:SB123914805204099085.html.

32 Ellen Messmer. "'Cyberwar' author: U.S. needs radical changes to protect against attacks," *NetworkWorld*, 7 Apr. 2010, www.networkworld.com/news/2010/040710-clarke-book-review.html (hereinafter "Radical Change").

33 *Id.* (reporting that the U.S. electric power grid already endures hundreds of thousands of probes per day); Fehrenbacher (stating that the 40 million smart meters installed globally have already seen a number of security breaches).

34 Messmer.

35 Mylrea.

36 "Cyberwar: War in the fifth domain," 7 Jan. 2010, *The Economist*, www.economist.com/node/16478792 (hereinafter "Fifth Domain").

and overall investment into smart grids runs in the tens of billions for some countries.[37]

In addition to the potential for extensive physical destruction and immediate financial loss, the threat of future cyber attacks undermines confidence in existing and new technologies like smart grids and, in turn, in the reliability of electronic, financial and health resources. This loss of confidence alone could cause tremendous societal and economic upheaval.[38] The development of smart grid use with nuclear reactors (and nuclear weapons facilities) creates even greater risks and potential damage. Beyond traditional attack and defence strategies, cyberwarfare might also entail attacking an entity or country's internal systems in order to temporarily distract or hamper them, as opposed to directly damaging them.[39] A country might choose this kind of cyber attack if, for example, it wants to disable allied support of a targeted opponent long enough to achieve a specific objective.[40]

Unique Features and Impact of Cyberwar

Although cyberwar could resemble traditional warfare in some ways, the unique characteristics of cyberspace bring new and unforeseen dimensions as well. Because systems in cyberspace are linked by computers and communication networks, the disruption caused by an ICT-based attack goes beyond the failure of a single system and often beyond national boundaries. Many data transfer processes affect more than one country and many Internet services are based on services from abroad; for example, host providers may offer webspace for rent in one country based on hardware in another. Even short interruptions to services could cause huge financial damages to e-commerce businesses. Civil communications networks are not the only systems vulnerable to attack, the dependence on ICTs is also a major risk for military

---

37 *Smart Grid: Hardware and Software Outlook*, Zpryme, 2009 at 2, www.zpryme.com/SmartGridInsights/2010_Smart_Grid_Hardware_Software_Outlook_Zpryme_Smart_Grid_Insights.pdf (stating that the U.S. smart grid industry was valued at $21.4 billion in 2009 and will reach an estimated $42.8 billion by 2014); Jonathan Weisman and Rebecca Smith,"Obama Trumpets Energy Grants," *The Wall Street Journal*, 28 Oct. 2009, http://online.wsj.com/article/SB125663945180609871.html (reporting President Obama's announcement of $3.4 billion in stimulus grants for advanced electricity grid projects).

38 Fifth Domain.

39 *See e.g.*, *Id.* (stating that "the more likely use of cyber-weapons is probably not to bring about electronic apocalypse, but as tools for limited warfare").

40 *Id.*

communications. Unlike more traditional combatants, cyber offenders do not need to be present where the effect of the attack occurs or even where it appears to originate. And while carrying out the attack, the offenders can use anonymous communication and encryption technology to hide their identity.[41]

Moreover, software tools, which are widely available over the Internet, are being used to automate attacks. With the help of such software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to more computers – e.g. through a botnet – s/he can increase the scale still further. For example, analysis of the attacks against government websites in Estonia suggests that they were committed by thousands of computers within a "botnet" or group of compromised computers running programs under external control.[42] Botnets also make it more difficult to trace the original offender, as the initial traces only lead to other members of the botnet. Current analysis suggests that up to a quarter of all computers connected to the Internet could be infected with software making them part of a botnet.

Software tools also simplify attacks, allowing less experienced computer users or less advanced military outfits to commit cyber attacks. In addition, ICT-based attacks are generally cheaper than traditional military operations and can be carried out by even small states. Now, even a state with historically weaker military capabilities has the capacity to severely cripple critical infrastructure through cyber attacks. This potential for asymmetry makes cyberwar appealing as a strategic way to level the playing field in otherwise *David versus Goliath scenario[s]*. The fear of cyberwar, reinforced by the actual (albeit limited) occurrence of cyber attacks, undermines public confidence in ICTs. Thus, the potential psychological ripple effect of cyber conflict could have widespread implications for disrupting the effective use of new technologies and hampering progress in many sectors.

---

41 *CERT Research 2006 Annual Report*, Carnegie Mellon University, Software Engineering Institute, at 7 *et seq*., www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

42 *Understanding Cybercrime: A Guide for Developing Countries*, at 72, International Telecommunication Union, April 2009, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (hereinafter "Understanding").

3 Societal Dependencies and Trust

3.1 Modern Societies' Dependency on ICTs and the Internet

By Jacques Bus

Computers and information technologies have been with us since the second part of the last century and the Internet started only 38 years ago as a communication network in the ARPA (DARPA) project. However, only in the last 15 years, due to the invention of the World Wide Web (we will call for convenience the combination of Internet and Web in the rest of this paper "the Internet"), the Internet has permeated the economy and social life with dazzling speed. We can currently enjoy communication and social networking anytime, anywhere; we have access to practically unlimited information; we can discuss and socialize with people all over the world; and we compare and order services and products from a comfortable chair at home at any time we want.

According to ITU estimates for 2009, 25.9% of the world's population has Internet connection (which amounts to 1.8 billion people). People spend twice the number of hours per week on the Internet than they spend on watching television. There are 4.6 billion mobile phone subscriptions worldwide amounting to 67% of world population. Facebook alone claimed more than 500 million active users in July 2010 and Facebook, Myspace and Twitter attracted together 220 million active visitors in July 2010. One of the most important changes world-wide is the transformation of the mobile phone into an Internet phone, replacing the PC as the favorite device for connecting to the Internet. Already 9.5% of the population worldwide has mobile broadband.

While the Internet has already changed modern society in essential ways and at a truly global scale there will be much more to come. In many publications[43] we read future scenarios on how the world may look like 25 years from now. Identity tokens used for access to public transport, health records, access to government services and networked services will become common. Social networking will expand and find new, more effective and more exciting applications. Data linking will bring new information services that will help researchers to do more effective research, travelers to better enjoy their journeys, citizens to understand administrations' rules and politicians'

---

43 *Trust in the Information Society: A Report of the Advisory Board RISEPTIS,* www.think-trust.eu/; David-Olivier Jaquet-Chiffelle, ed., *Identity Revolution: Multidisciplinary Perspectives,* FIDIS, May 2009, www.fidis.net/resources/identity-revolution/.

motives, etc. And agents and policy-based processes will take away from us much of the administrative burden, like making appointments, preparing for meetings and complying with jurisdictions.

The ICT-based societal revolution will lead to essential changes in the balance of power, at the national level where citizens are having abundant information on the political processes which will be used in the democratic process, but also at the international level. Access to the Internet is empowering citizens to be better included in economic and political life, and to understand situations and ways of life in other cultures. We have seen the way U.S. President Obama used the social networks in his campaign and we may expect that similar activities will be developed in the future to support governmental policy-making.

ICTs also allow international companies to organize themselves in ways that make optimal use of opportunities all over the world. This can all give a strong boost to economic development and growth globally, and particularly in low-cost countries. We see already large developing countries taking advantage and become important economic and political players.

However, as with every revolution in history, together with the opportunities and benefits there always is a downside.

Information and communication infrastructures and services have become a critical part of our economies. They are extremely vulnerable, as the many attacks reported almost daily demonstrate. Most of our other critical infrastructures, e.g. energy, water, transport, financial systems are heavily dependent on ICTs for communication and control. There is therefore a high risk of accidents or deliberate attacks on these critical infrastructures that may potentially lead to chaos and enormous economic losses. This includes intrusion and attack on systems and databases of national security agencies.

This vulnerability of our societal ICT infrastructure makes it an easy target for “cyberwar” or “cyberterrorism” which creates a threat for geopolitical stability. Deliberate organization of attacks on critical systems of one state’s society with approval, support or control of another state is sometimes called “cyberwar”. It should be clear though that the word “war” in this context may create confusion as it is in many ways not comparable with what most people have in mind when talking about war: being long-term destruction of physical infrastructures and massive loss of lives.

In the past few years several attacks happened where the term "cyberwar" was used; for example in Estonia,[44] Georgia, South Korea, US. It sometimes started with amateurish psychological "warfare" with propagandistic goals, which in a second phase involved cyber attack specialists (criminals or otherwise) in a full-scale campaign through botnets launching DDoS attacks on the social and economic infrastructure. In other cases the cyber attacks were executed just before or during kinetic war actions. Up until now the destruction caused by the cyber attacks was mostly limited and capacity could be restored after a few days, with no mention of loss of lives directly due to the cyber attacks.

The roles that states have played in these conflicts are mostly unproven. But this proves the urgency to come to international agreements on restraints in and defence against cyber attacks and for international cooperation to bring it under control. It is clear that the old doctrine of deterrence in the Cold War is not easily applicable in cyberspace. It is not well understood what such deterrence would consist of and, more importantly, the enemy is difficult to identify (lack of attribution and use of proxies).

Let us leave aside the political debate on the term "cyberwar". There is no doubt that cybercrime is becoming a very worrying issue. The number of malicious and criminal code threats is increasing exponentially. In 2008 alone, Symantec detected 1.6 million threats, being 60% of the total of detected threats in all years before 2008. More than 8 million US residents were victim of ID theft. The average cost of a data breach in the US was estimated at USD6.7 million. And in February 2010 it became known that 750,000 company computer systems world-wide were infected and taken over by botnets. Amit Yoran, a former US official, suggested that companies are simply not prepared for defending themselves, though this was later downplayed by the US security industry.

Howard Schmidt, (Special Assistant to the US President and Cybersecurity Coordinator), acknowledging the increasing problem of malicious use of the Internet, however, gives clear priorities. He rejects the term "cyberwar" as "a terrible concept". He does not see winners in that environment and proposes to focus on online crime and espionage.

Despite the different opinions, there is general agreement that there is reason for alarm about the security and trust in the Internet. Current trends risk increasing fear for and rejection of the new digital world by citizens. It may have huge economic

---

44 See also Kertu Ruus, "Cyber War I: Estonia attacked from Russia," *European Affairs*, Vol.9, No1-2, 2008, http://findarticles.com/p/articles/mi_7054/is_1-2_9/ai_n28550773/.

consequences if politics and technology are not able to deal with these negative societal developments.

In her speech of 21 January 2010, Hillary Clinton, US Secretary of State, emphasized the importance of an open and free Internet for global cooperation and development. She referred to the "Four Freedoms" of Roosevelt – freedom of expression and worship, and freedom from want and fear – and the important effect of the Internet on these freedoms, particularly freedom of speech. The Internet has led to a revolution in information exchange and social networking. It has great potential for creating more wealth for everybody, in particular when "Freedom to connect" is fully recognized. It has however also led to increasing global crime and the creation of fear, which need to be contained.

Politicians have recognized clearly the enormous importance of the Internet in the global geo-political arena. They understand that citizens expect governments to give them safety and protection while national jurisdiction and borders are no longer giving this in the way they did before. Consumer law as currently applicable in many countries, as well as product and service liability, do not work in a world where customer and supplier are in different and non-cooperating jurisdictional areas and services are delivered through ad hoc chains of sub-services using data from clouds spread all over the globe.

World leaders are facing enormous and unparalleled challenges. Climate change and rapid changes in global economic power and energy security, to name a few, need political attention as well as the risks created by global digital connection. We will need strong and visionary global leadership to solve all these problems.

In all this, most important is to use what we have learned through history about societal structures and values, security, trust and international relationships. We must engage in a global transformation to transpose our cultures, societal values and strengths, and international cooperation processes so as to be usable in a world that recognizes the digital networked reality.

Necessity for Trust

The concept of Trust and its role in society

"Trust pervades daily life. If we take only a small sample from the bewildering array of occasions where trust plays a role, we can see that, of all social phenomena, it is surely

one of the most vital. But this very centrality brings problems for the study of trust – How can one even begin to understand such a protean social force?"[45]

Trust and trustworthiness are concepts which are at the basis of human existence. We use them intuitively and their assessments are invariably context dependent. But when we transpose these concepts to a digital environment, we can easily run into trouble.

Luhmann[46] explained trust as a mechanism that reduces complexity and enables people to cope with the high levels of uncertainty and complexity of (contemporary) life. Thus, trust expands people's capacity to relate successfully to a real world whose complexity and unpredictability is far greater than we are capable of taking in. In this sense it is a necessary mechanism for people to live their lives: to communicate, cooperate, do economic transactions, etc. It enriches the individual's life by encouraging activity, boldness, adventure, and creativity, and by enriching the scope of the individual's relationships with others.

Seen from another perspective one could say that trust is the expectation of benign behaviour towards the trusting party in a certain situation. As explained by Hardin:[47] "Trust is in the cognitive category with knowledge and belief. To say I trust you is to say nothing more than that I know or believe certain things about you that make me believe you are trustworthy to me and will act "benignly" even in unpredictable circumstances."

Trust is a three-part relation (*A trusts B to do X*). The evaluation of the trust *A* has in *B* to do *X* plays an important role in the decision of *A* to partake in any transaction, exchange or communication with *B*. By reducing the complexity and perceived risk, trust effectively facilitates economic activity, creativity and innovation. Trust is highly context dependent. It is contingent on: time (one could easily lose trust in someone, but also the concept changes over time); history and memory; place and situation; culture; role (private or professional); emotions; and a number of other variables (for example, sociological considerations like reputation, recurrence and recommendation).

---

45 Kieron O'Hara, *Trust: From Socrates to Spin*, Icon Books, Cambridge, 2004 at page 10, http://eprints.ecs.soton.ac.uk/9361/.

46 Niklas Luhmann, *"Trust: A Mechanism for the Reduction of Social Complexity", Trust and Power*, New York: Wiley, 1979 at 4-103.

47 Russell Hardin, *Trust and Trustworthiness*; Russell Sage Foundation Series on Trust, Vol. 4, 2002.

It is clear from the above that trust is a concept that can be strengthened incrementally in a given situation and between two given parties. More information, maybe through other sensors or via relations, can help to strengthen trust, as well as a longer duration of a successful relationship.

In general, we would in this discussion consider parties *A* and *B* to be human beings. This does not exclude the possibility that these humans act on behalf of organizations or groups. In practice, however, many people would also talk about trust in other entities, e.g. the government, a company, a system or service, a database or an information service (e.g. a paper, technology blog), or maybe even a virtual entity like a software agent. Hardin would call this "confidence in the entity's actions, behaviour or integrity". This could be created, for example, through accountability, transparency, assurance and liability, audits and reputation, or knowledge about intentions of the entity.

The concept of trust as social capital, or "social trust", has been discussed and developed by Fukuyama,[48] Putnam[49] and other experts. This is a statistical concept expressing the opinion of people on the trustworthiness of their society in all its aspects, or maybe more precisely: the confidence of people in the government, institutions, laws, systems, etc. of society. It appears that there is a strong correlation between high social trust and high economic growth and prosperity.

We will mostly use the word "trust" also where Hardin would call it "confidence". However, for further discussion it is important to distinguish trust between persons that make use of networked digital systems and services in their interactions, and trust or confidence of a person in a non-human entity or institution.

The introduction of digital technology has revolutionized human communication and cooperation by introducing a new intermediary consisting of a complex set of technology-based "institutions" (including networks, digital services, data bases, social networks). In dealing with trust between human actors we must therefore also consider the aspect of trust (or confidence) in this technology infrastructure.

---

48 Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, 1995

49 Robert D. Putnam, Robert Leonardi, and Raffaella Y. Nanetti, *Making Democracy Work: Civic Traditions in Modern Italy,* Princeton University Press, 1993

Nissenbaum[50] discusses only trust between persons making use of networked digital systems for their communication and lists factors to which tendencies to trust (or not to trust) are systematically responsive:

1. History and reputation.
2. Inferences based on personal characteristics: e.g. virtue, prudence, loyalty, desire for good opinion of others, behaviour, clothing.
3. Relationships: mutuality and reciprocity, family, be in the same boat, having common ends.
4. Role fulfillment (pilot, bus driver).
5. Contextual factors (groups and communities – publicity; reward and punishment; norms; trust insurance or safety nets like liability or consumer law).

A number of these issues, in particular 1 and 3, have aspects of "Trust as encapsulated interest" as defined in Hardin[48]. It is in the interest of the trustee to act benignly so as, for example, not to lose reputation which could lead to breaking the relation by the truster (e.g. a pilot who loses his reputation might lose his job). She also lists obstacles to trust online:

1. Missing identities (but note the right to anonymity)
2. Missing personal characteristics (but note the right to privacy)
3. Inscrutable contexts (unknown and confusing which creates obscurity, but also liberates)

The third point could be seen simply as higher complexity online. It allows more freedom, of course, but, at the same time, for a proper transaction or communication one will need to build even more trust and hence dependency. Nissenbaum also notes that security does not bring trust. If there is security, there is no need for trust. However, trust enables people to live in a richly complex insecure world and more security reduces the richness and complexity. Other authors see security at one end of the trust scale with completely unfounded (naïve) trust at the other end.

The fact that through the global information infrastructure trust (in strangers) is growing with more knowledge (about them) brings the Economist to state: "The desire of so many people, given the chance [...] to live in countries other than their own,

---

50 Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?" Boston University Law Review, Vol. 81, No. 3, June 2001 at 635-664, www.nyu.edu/projects/nissenbaum/main_cv.html .

makes nonsense of a long established consensus in politics and philosophy that the human animal is best off at home." [51] And more: "The error of philosophy has been to assume that man, because he is a social animal, should belong to some particular society."[52] Nevertheless, this could be too quick a generalization of minority behaviour, as those who travel more and further than the well-assured trustworthy holiday trips organized by liable agents at home are still a very small minority.

Yet, globalization, driven clearly by new ICTs and the Web, creates understanding and hence more trust through spreading information on history and reputation of societies, characteristics of societies and the lives of persons living in certain societies, and allowing easy worldwide communication. This may indeed lead to further erosion of the concept of "the human animal is best off at home". It may well lead to the need for a completely new view on societies and their cohesion and the role trust must play in this.

Trust in the Digital Society

As mentioned above, we must distinguish between:

- Trust between persons in a society which makes extensive use of digital technology for communication and transactions.
- Trust or confidence of people in the infrastructure of digital networks and systems they use for services, communication, data storage, computation, etc.

Let us start with the first point.

The problems with trust (between persons) in the digital society in comparison with the "old society" relate particularly to:[53]

- The transformational change in the way data is collected, stored, processed, made available and protected. Not only is data collected and stored that is produced by persons with a view to communicate and store it, but, in particular, data is collected on behaviour through surveillance (from walking in the street to visiting websites or opening web ads).

---

51 "The Others," *The Economist*, 17 Dec. 2009, www.economist.com/node/15108690.

52 *Id.*

53 *See* Nissenbaum.

- Identification, reputation, authentication and accountability have a different meaning on the Internet. One needs to prove attributes, provide secrets or biometric information to convince someone of one's identity. Reputation can be easily ruined through spreading embarrassing or false information, which is extremely difficult to correct. The possibility to hide in other jurisdictions undermines accountability and transparency significantly if there are no international agreements on law enforcement and extradition.
- Increase of complexity, incomprehensible technology with insufficient assurance through certification and standardization, and lack of transparency of the processes and methods of data collection and use have created an inscrutable context, which undermines the trust that needs to be established between persons in the digital environment. People may be perplexed with what happens around them and often have no clue about what data is collected on them and how it is being used.

Trust is easier to establish when the identity and/or other authentication information (credentials, attributes or claims) about the third party are known or can be confirmed (possibly by a trusted third party). Reputation and other knowledge from the Web or from friends in social networks may give additional trust. Moreover, citizens will have more trust in a transaction with a third party if they have control over the exposure and exchange of their data to that third party. It will also be increased through transparency of operations of data collectors and processors, and through reputation of such entities.

But, bringing us to the second point, such trust between people can only be obtained in our technological world if one can have trust in the systems used to communicate, to exchange data, or to confirm identity and other information like reputation or credentials. To use the Internet, citizens must have confidence in the tools, systems and infrastructures they use for their transactions and communication. We call a system or service *trustworthy* to a certain level if a person can have a certain degree of justifiable trust that the system or service will deliver in accordance to its description and promises, and that it will not perform actions that are not described under various circumstances. Justifiable trust can be given through accountability (product liability), transparency on data processing and storage, technical system certification, and ex-post audit ability. It can also be strengthened through provision of comprehensible and useful tools and mechanisms to enable confirmation of claims on credentials, reputation or identity. People are in need of services and tools that can help them to create and strengthen trust in quality of service, security, resilience, data protection and privacy, in accordance with predefined and understandable policies. These could be provided through third-party service providers as well as public authorities.

As is argued by Vitali Tsygichko,[54] an important special role in modern society is played by automated information systems (AIS) that become more and more integrated in public administration systems across all sectors of a national economy. AISs constitute the core of decision support systems in virtually all socio-economic organizations. It is not only the efficiency of public authorities, of the economy and voluntary organizations but also the national security that are largely dependent on reliability of AIS performance.

It is obviously extremely important to consider the trustworthiness of these systems. This relates primarily to validity of their underlying models, the reliability of its soft- and hardware facilities, the level of professional qualifications of the staff maintaining the system, and the effectiveness of measures for its protection from external threats.

Following Tsygichko's argument, trustworthiness of AISs need development of a set of requirements and metrics for security, reliability (including the underlying model as a representation of reality) and data integrity. A measure of security breach risks can be used as one assessment criterion. **Risk management** is defined as processes involving risk identification and analysis and decision-making including maximization of positive and minimization of negative implications of risk event occurrence.

In addition to the technical means needed for building trust, we will need rules and regulations and societal acceptance. Citizens will trust the handling of their personal data within their society if: privacy and personal data protection regulation is respected and enforceable; organizations comply with citizens' perceptions of a culture of accountability through proper consumer protection and redress regulation; regulation on auditing and transparency; and clear responsibility allocation in the chain of actors in a transaction is implemented.

At a general policy level, a trustworthy ICT infrastructure can only be created and sustained with a proper and fair distribution of incentives over the total value chain.

Transparency and accountability need to ensure fairness and enforceability. The problems with liability of systems and, in particular, the software and data integrity parts, need to be addressed. This could lead to development of a system of insurance of security breach risks, which in turn will boost development of measurements and tools to enable risk assessments. All this could eventually lead to a largely self-regulated and sustainable system.

---

54 Vitali Tsygichko is an associate member of the PMP InfoSecur and participated in these discussions.

An essential requirement for building trust between people using the Internet is the development of a globally interoperable trustworthy system for **Identification and Authentication.** The development of reliable e-ID cards and passports by governments according to standards that are agreed to worldwide is one example taken up by many countries. But for global e-transactions we need interoperable claim and credential management on the Internet that ensures compliance to privacy rights. Accountability is essential for the Internet economy and can only be achieved through effective liability of persons and organizations for their public and contractual actions. The latter is normally done through proving credentials, demonstrating attributes or using secrets that are only known to the person. One can use different secrets, credentials or attributes in different situations, leading to different "identities". Meta-level standards for identity claim management have been proposed by Cameron, Posh and Rannenberg.[55]

The Internet, with its many different social networks, also provides the opportunity for people and organizations to build their narratives, circles of friends and reputations in various communities. In the terminology of the FIDIS project[56] this would lead to "partial identities" of a person. When in situations requiring accountability, this can be linked in a privacy-protecting way to identification, authentication and digital signatures. It could also help in providing more trust in the Internet as a mechanism for social and economic activities.

Summary

We discussed the relevance of and different views on trust in our society. In particular we discussed the changes and problems that have been emerging as our society becomes more and more dependent on digital communication and transactions through the Internet. The lack of sufficient identification respecting the need for anonymity in some cases, the missing experience of personal characteristics together with the need for protecting privacy and, last but not least, the inscrutable context created by the technology infrastructure used for our communications, has deprived human beings of essential mechanisms to create trust to enable their living and creativity in the globalized society.

---

55 Kim Cameron, Reinard Posch, and Kai Rannenberg, *Proposal for a Common Identity Framework: A User-Centric Identity Metasystem,* Joint 'ICT Security' – 'ICT for Government and Public Services' Workshop on "Identity Management in the Future Digital Society, 14 Oct. 2008, www.identityblog.com/?p=1048.

56 "About the FIDIS Network of Excellence," www.fidis.net/about/.

We must therefore develop new trustworthy mechanisms in the digital environment that enable people to build trust between each other, independent where they are or how they meet.

We must ensure secure and trustworthy communication networks; information systems that give assurances on compliance with data protection and privacy law; a trustworthy global and interoperable framework for identification and credential/claim management; and services that satisfy proper liability and consumer protection laws. This technology must be designed and developed with trust, security and privacy in mind and enable law enforcement and transparency, while law and regulation must be developed with the technology trends and potential in mind.

Public and private sectors must work together at the international level to build a well balanced infrastructure of technology and law/regulation that will give citizens trust to use the opportunities of the new digital world.

In doing so, humanity can obtain, up until now, unforeseen opportunities to communicate, cooperate and have economical transactions at a global level based on trust mechanisms, similar to what we have known in the past in small communities through direct human interaction. This will constitute a firm step towards global stability.

3.2 Socio-economic Implications of Cybercrime

By Jacques Bus[57]

Digital services provision, and in general the digital infrastructure that is being developed for our society, has enormous positive potential. At the same time, as all technology, it can be used for malicious activities. We may distinguish the following four problem areas in relation to socio-economic issues:

1. **The global character of the digital space**: Appearance of cross-border services and communication on the Internet creates a number of economic and social trust issues and issues of national security that were up until now dealt with at the borders of nation states (import and export control, passport control, customs, aggression between nations, etc.) or within the state by local or national police actions against registered citizens. The negative consequences of the non-existence of border controls in digital space have hardly been addressed in any substantial way, neither at the nation state level nor at the international level. It is clear, however, that it facilitates crime by creating a kind of immunity for criminals, partly because action on the Web can be difficult to attribute to actors, and partly because actors are in states that give them protection from international law enforcement.

2. **Complexity of services:** Transactions and services on the Web are more and more set up as ad hoc chains of sub-services, which are spread over jurisdictions and using data from all over the cloud. The sub-services or data can fall under various, even contradicting jurisdictional regimes. Consumers have difficulty realizing this and also understanding the consequences. States can no longer guarantee product liability and protection of their consumers in the way done up until now. They will need international agreements and law enforcement cooperation to deal with this. Moreover, services need to ensure transparency on the service chain and be responsive (automatically) to conditions consumers set on it. The current situation, together with point 1, opens up widely for untraceable deceit and fraud. And presently states can give no protection to this.

3. **Social networks and chat rooms:** These are often used for making connections with malicious motives, particularly focused on children or the elderly. This is not new. Scams and deceit have always existed. However, poor authentication

---

57 The author would like to acknowledge the contribution of Udo Helmbrecht and his team at ENISA (European Network and Information Security Agency).

and lack of secure and privacy-protecting proof mechanisms for credentials (like name, birth data, age, gender, employment data, passwords) make it all very easy and profitable. Viruses have also reached social network sites, as it is there where trust can be used as a vector. Success rate of attacks using social networks is very high. Phishing is the number one threat to banks, but banks do not yet offer services to authenticate themselves to their clients.

4. **International organization of crime:** It has been reported in many places in the past few years that international crime not only moves to the Web to implement their criminal intentions, but that an international black market is working for criminal tools (botnets, tools for phishing, viruses, etc.) and stolen data (personal information, credit card data, company secret information). Crime on and using the Web is getting better and better organized internationally, widely spread over jurisdictions, including ones with very weak judiciaries, and very much focused on financial gains. There are many examples of this development. The FTC closed a semi-legal scareware company in March with an annual turnover of USD 180M. There are money-back guarantees on viruses, technical support and "do-it-yourself" kits for criminal acts. The Zeus banking Trojan costs USD 700 (USD 4000 for the latest version) on the black market (Zeus is used to foil authentication schemes such as two-factor schemes and the Mastercard secure-code scheme). There are several layers of legal and semi-legal suppliers that make profit from the underground economy.

Studies and statistics give sometimes staggering figures on the societal and economic losses in relation to these illegal activities. These can go as high as USD 1 trillion[58] globally, which would amount to almost 2% of global GDP. Boston Computing Network estimated that American business lost more than USD 7.6 billion as a result of viruses during the first six months of 1999. German figures on financial loss of phishing are estimated at €15 million per year and credit card losses at €155 million.

In general, most figures on economic loss are based on assumptions that are debatable, and are necessarily extrapolations of what is known, whilst many problems are not publicly reported. The conclusion can nevertheless be that the socio-economic cost of cybercrime is very substantive and often underestimated by those who have to

---

58 "McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property," McAfee Press Release, Feb. 2010, www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html; see also Unsecured Economies Protecting Vital Information, McAfee, 2009, http://resources.mcafee.com/content/NAUnsecuredEconomiesReport

make decisions on investments in security measures. The return on security investments should be looked at far more seriously.

Fighting cybercrime requires the need to assign liability for actions in the digital environment. This includes the sub-actions in dynamically created internationally spread service. Legal cooperation and diplomacy is needed at international high political levels to define common policies and procedures that create reliability of and liability for services and public and economic actions.

Technical development is required to find solutions that on one side preserve the global non-divided network, to which businesses and consumers have access for work, communication and information, at home and when travelling, in ways that ensure compliance with the laws that apply at all instances of the activity. On the other side, people have the right to private life on the Web, and hence should have the possibility to act on the Web within the limited secure trust circles they choose themselves in certain situations and with guarantees from providers that their data exchanges are not used for other purposes.

Unfortunately, we currently are seeing the development of an economy of private data that goes in an opposite way. Data collecting and processing companies are getting their profits solely from a business model around private, customer data. Consumers may think that they are customers of these service providers and hence they may be held responsible for the service. But in reality, as the consumer does not pay anything to these companies, actually they are only the product. The marketing companies, data analysts, profilers, advertisers, and other companies are the REAL customers to which Social Network Sites, Service Portals, etc. sell the data of the consumers.

Actually private life seems to become the real victim of developments in the socio-economic space related to digitization and networking. The price of data storage is decreasing very rapidly and eventually data will be stored without limits in quantity and time. This will have a profound impact on how we interact, and will also create new crimes in the future (privacy breaches, unauthorized profiling, unauthorized data mining) as well as new ways of political control. Much of this could be against currently existing constitutional rights and the impact this will have on social, economical and political stability in society is hardly discussed.

In addition to the possible effects of the digital environment on crime and human rights discussed above, a completely different danger for society and economies relates to the extreme vulnerability of the future digital societal infrastructure. Societies as a whole may face severe economic and social losses when their communication networks or other critical infrastructures are attacked and disrupted,

whether by criminals (for extortion), by terrorists for creating fear and instability, or by other states as part of war or deterrence. The potential of states to act against such attacks is practically limited to defensive actions. More offensive strategies like deterrence or counter-attack are difficult to implement as the attacks are often not attributable and are often initiated in unknown places or rogue states. Technological development, if not giving sufficient attention to security and trust in networks and systems, will increase these problems and may lead to national and international conflicts becoming uncontrollable in the future.

Finally, an essential and additional element that must be looked at is the longer terms risks for society. Attacks can last a matter of seconds with rather extensive effects. The societal trust lost in these seconds may take years to rebuild. Undermining trust between people, between people and businesses, between citizens and their state, and between states themselves can have devastating effects on societies and global stability in the long term. It will be an obstacle for future effective economic growth, which in the current post-crisis economy depends heavily on the growing use of ICTs. We cannot afford stagnation in this area due to the loss of trust.

Network and information security, including authentication, in the digital environment must assure the safety of citizens (physical, economical and private). Trustworthy ICT systems, infrastructures and institutions will assure a level of social trust in our societies which is essential for economic prosperity, as has been shown in many studies.

Societal instability and economic damage (in terms of economic growth) is difficult to measure but can be very significant. It urges for preparedness and strong protection, as well as quick recovery and self-healing of systems.

Summarizing, we can say*:*

The global character of digital space, with weak identification of users and insufficient attribution of actions, the complex internationally spread services, the global development of social network sites, and the emerging international crime networks and markets raise serious worries about the rise of cybercrime and hence the sustainability of a stable society as a basis for personal development and economic prosperity.

The vulnerability of our societal ICT infrastructures and the limitlessness of data collection and storage threaten personal freedom and international stability.

The trust citizens have in society and government to protect their peace, safety and prosperity gets eroded by the dangers and uncertainty raised by technical developments, with potentially heavy economical losses.

We therefore urgently need global political action to address these problems, based on solid analysis of the technological, societal, economical and political trends and consequences.

4 Technology Trends and Threats

4.1 Current Potentials, Trends and Threats

By Axel Lehmann, Vladimir Britkov, Jacques Bus

Driving forces for product innovations are technology "pushes" as well as market "pulls". In this respect, analyses of future directions and potentials of ICT innovations have to consider current and expected technological advances, as well as trends of future consumer or market demands. Therefore, the first three sections of this chapter are addressing those trends and demands accordingly followed by an analysis of major threats and some concluding remarks.

To start this chapter with a summary of the following analyses and evaluations, we assume that the expected technological innovations will not only enable rapid advances of new micro- and nanotechnologies, but also the development of large-scale integrated sensor and computing devices, of new network and communication technologies, and of innovative services and applications. These innovations will also enable two major directions of evolutions:

- convergence of current single computers and user mobile phones to single portable, mobile multi-use computing and communication devices; and
- evolution of current Internet, web technologies and services towards a future Internet. The "internet of things" which will be characterized by massive communication and mobility of, as well as between, individuals and all kinds of devices and objects ("things") will be one step forward towards an efficient, reliable and trustworthy future Internet.

These technological advancements will be reinforced by market and consumer demands for the development of new ICT products, services and applications. According to a study published by Forbes, sectors of entertainment and communication, energy and health care will be especially driving forces and major application domains of innovative ICT products.[59]

---

59 Robert Krysiak, "Semiconductor Mega-trends in 2010," *Forbes*, Jan. 2010, www.forbes.com/2010/01/04/stmicroelectronics-healthcare-entertainment-technology-cio-network-semiconductors.html.

In this respect, the following three subchapters will summarize major impact factors on future ICT developments and their consequences: technology trends, market and consumer demands, and "Internet of things", while basic chances, threats and challenges of these ICT innovations for our private and public life are summarized in the last two subchapters.

Technology Trends

Without any doubt, in the current decade miniaturization and digitization have significantly contributed to a big step forward towards a "digitized world" in which all kinds of data, information, and knowledge are stored, transmitted and processed in digital form. Trend analyses of further developments of its current base technologies, semiconductors, indicate that Moore´s law of "doubling the number of transistors per square inch every two years" is probably still valid for at least another decade. Current design and fabrication techniques allow integration of some billion transistors on a single chip. Even if in the long term current semiconductor technologies will be replaced stepwise by new technologies, such as biotechnologies or quantum computing, these general trends of increasing miniaturization and digitization, of enlarged functionality and applicability will continue and enable further enlargement of ICT and of ICT-based products and applications.

In this regard, four major areas of future digital system developments and organization principles have to be considered in the context of hardware, firmware and software advancements:

- Single and multiple computer systems.
- Communication networks, protocols and services.
- Nanotechnologies, materials sciences, sensors, actors and embedded systems.
- Decentralized operation and organization mechanisms for digital systems.

As very large scale integration of transistors per chip area plus increasing clock frequencies created overheating problems, current **microprocessors** are designed as multi-core processors working with reduced clock frequencies, but increased performance enabled by parallel processing on chip. Further processor innovations will be enabled through multi-layer semiconductor technologies, increasing number of core processors and lower power consumption per chip. This will result in significant performance improvements through multiple-core processors, multiprocessor systems, further increasing cache and main memory capacities, and system-on-a-chip developments. These trends will increase performance of the whole range of computers ranging from single-chip computers and embedded computing components

up to supercomputers. As communication and switching networks will also advance, all kinds of structures and architectures of interconnected computers will be available.

In addition, through improved miniaturization techniques, fast external storage devices with higher storage capacities and minimized access times will also be available. Along with advanced architectural approaches and software techniques, massive parallel execution of complex software applications will be feasible. In parallel, through development of new low-power technologies and batteries, the mobility of computers and all kinds of computing devices will be significantly improved, or facilitated.

In the area of **communication networks, protocols and services,** major innovations will result from permanent improvements of wireless and satellite communication techniques offering higher connectivity and increasing bandwidths. One major trend concerns the dynamic formation of virtual networks, e.g. virtual private nets.[60] This technique, which is already applied, offers the timely limited formation and usage of application and user-oriented networks consisting of selected network components and services.

Another trend towards higher flexibility and usability of existing computing and communication infrastructures is concerned with the formation of overlay networks. Currently as a major research topic, this technical approach is seen as an efficient approach to overcome current limitations of existing IP/TCP protocols and to evolve from IPv4 to IPv6, which are important steps to an enlarged usage of the Internet, and an "Internet of things". Technical advances in both directions are prerequisites for further innovation of internet technology and applications. The tremendous growth of the current Internet – especially concerning the variety and number of objects connected to the Internet – requires on one side a significant expansion of the current address space of internet objects (IPv4) towards IPv6.[61] Therefore, special transformation techniques allowing a scalable transition between these two standards have to be developed. On the other side – and concurrent with the evolution from

---

60 James Henry Carmouche, *IPsec Virtual Private Network Fundamentals*, Cisco Press, 19 July 2006, www.ciscopress.com/bookstore/product.asp?isbn=1587052075.

61 S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," The Internet Society, Dec. 1998, www.ietf.org/rfc/rfc2460.txt; Walter Goralski,, "The illustrated Network: How TCP/IP Works in a Modern Network", The Morgan Kaufmann Series in Networking, 2008, www.freshwap.net/forums/e-books-tutorials/120250-illustrated-network-how-tcp-ip-works-modern-network.html.

IPv4 to IPv6 – the development of future standardized IP/TCP protocols has to be provided to enable communication between all kinds of objects through a "future Internet". Though both directions of research still require concrete solutions, it can be assumed that those technical foundations for a future internet will be in use in a few years from now, offering advanced and new capabilities for Internet applications, e.g. for the "Internet of Things".

In addition to the above-mentioned ICT system development trends, rapid technical and production advancements in nanotechnologies, materials science, and in specialized digital components – like in semiconductor-based sensors, actors or embedded systems – have to be considered when analysing future trends and threats of ICTs. These advancements will result in ICT-components, such as:

- Tangible user interfaces.[62]
- Polymer displays.
- Digitized clothing (Wearable computer).[63]
- Passive and active sensors (RFID technologies[64]).
- "Ambient intelligent"[65] or "Smart" systems.

Along with these technical advancements, improved and new **firmware/software products, services** and organization mechanisms will offer opportunities for improved

---

62 Hiroshi Ishii, "The tangible user interface and its evolution," *Communications of the ACM*, Vol. 51, Issue 6, June 2008, http://portal.acm.org/citation.cfm?id=1349026.1349034.

63 Steve Mann with Hal Niedzviecki, *Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer*, Doubleday of Canada, Nov. 2001.

64 *RFID Adoption and Implications*, European Commission (Enterprise & Industry Directorate-General, ICT for Competitiveness and Innovation), DG Enterprise & Industry, The Sectoral e-Business Watch, Impact Study No. 07/2008, Final Report, Sept. 2008, www.ebusiness-watch.org/studies/special_topics/2007/rfid.htm;. Arun N. Nambiar, "RFID Technology: A Review of its Applications", Proceedings of the World Congress on Engineering and Computer Science 2009, Vol II, WCECS 2009, 20–22 October 2009, San Francisco, USA, www.iaeng.org/publication/WCECS2009/WCECS2009_pp1253-1259.pdf.

65 E. Aarts, R. Harwig, M. Schuurmans, chapter "Ambient Intelligence," in Peter J. Denning, ed., *The Invisible Future: The Seamless Integration Of Technology Into Everyday Life*, McGraw-Hill Companies, 2001 at 235-250; D. Wright, S. Gutwirth, M. Friedewald et al., *Safeguards in a World of Ambient Intelligence,* Springer, 2008, www.springer.com/computer/database+management+&+information+retrieval/book/978-1-4020-6661-0.

and added functionalities and services. These advancements range from various innovative software technologies (e.g. agent-based software development), service-oriented architectures (SOA), new web services, or management systems (e.g. for efficient data storage or data retrieval, for efficient load balancing) up to efficient use of grid-like infrastructures formed by huge networks of distributed computer and communication resources. Most relevant and far-reaching applications are grid-computing or cloud-computing[66] which open a new era of ICTs regarding its economics, performance, availability and reliability.

Besides all the technological advancements described above, especially two major, fundamental trends concerning **organization and operation principles** have to be taken into account when analysing essential trends and threats of ICT innovations: **virtualization and decentralization**. The permanent increase of functionalities and interconnectivity of heterogeneous digital components, on one hand, and the demand for their effective use, on the other hand, have led to the formation and operation of virtual systems, e.g. of virtual processors, of virtual storages, or even of virtual computers. In addition, the permanently increasing complexity of networked computer and communication systems and the usage of virtual networks as mentioned above often prevent effective operation based on centralized control. Instead, more and more operation mechanisms for decentralized system control are being applied, which have proved to be more flexible and effective compared to the centralized ones. Examples for the latter are agent-based software applications, or bio-analogue system control.

Realization and application of both principles together – virtualization and decentralization – have already led to new opportunities of efficient use of networked digital resources. Such networks can form "grids":[67] a computer grid consisting of networked computer nodes, a data-grid formed by interconnected distributed storage systems, or equipment-grids formed by specialized devices which can be remotely accessed. In case of cloud computing those networked and interconnected resources can be remotely accessed and used via providers. Besides these economical and performance benefits, risks have to be considered, too. The general challenge – and currently a major risk – concerns mastering the complexity of those systems, especially regarding safety, reliability, and security. With respect to current state of science, those networked systems – which we have already in operation – can neither be fully

66 Vladimir Britkov, "Grid and Cloud Computing," Paper to the World Federation of Scientists Permanent Monitoring Panel on Information Security, May 2010 (hereinafter "Britkov").

67 Britkov.

verified with respect to their correctness, nor completely validated with respect to specific applications, nor fully tested due to their tremendous state space. This situation has not received enough attention up to now, though it shows a fundamental problem regarding ICT innovations.[68] Besides this challenge, further risks arise from the occurrence of faults and failures, as well as from sources for potential misuse and manipulation. These risks have to take into account an overall evaluation of these ICT innovations and much more research on countermeasures is urgently required.

Trends of Consumer and Market Demands

Already now, a major demand of markets and consumers address ubiquitous computing, communication, and information access – which means usage of digital devices and networking capabilities "everywhere at any time". High mobility of consumers on one side, and global distribution and availability of information and knowledge, on the other side, increase demands for improved or added functionalities of ICT products and of their efficient use. These demands will be permanently and substantially growing and generated by different markets. For example, there exists an increasing demand for locally distributed and time-independent cooperation in industries and economies.

All these demands are implicitly based on the assumption that we are going to live and work in a completely digitized world where each single object or each piece of information can be addressed and used at any time from any location. These consumer and market driven demands generate a significant "pull" for technological innovations, e.g. for effective use of multimedia or video applications, ubiquitous web access, computer supported cooperative work (CSCW), or the use of a huge variety of (web-based) services and applications. Beside new and useful ICT components and products, advances towards an "internet of things" might cause new social and governance issues as well as potential threats to safety and security. Therefore, these innovations and their implications have to be carefully analysed from the beginning – which is right now (see following subchapter).

---

68 Vladimir Britkov and Axel Lehmann, "Security challenges arising from innovations in information and communication technologies (ICT)," *International Seminar on Nuclear War and Planetary Emergencies*, 38th Session. E. Majorana Centre for Scientific Culture, Erice, Italy, 19-24 Aug. 2007 at 503-515.

As described above, current and future hardware/firmware/software advancements will enable new ICT-based products and innovative applications along these lines and for various application domains. Examples for such application domains are:

- Ambient assisted living (e.g. for the elderly).[69]
- Intelligent control systems (e.g. in transportation, logistics, aeronautics for navigation, energy-saving, etc.).
- "Intelligent" houses.[70]
- Health care.

While demands in the entertainment and communication sectors are mainly focused on ICT performance and economic aspects, other application domains like control or surveillance systems in the energy or health care sectors have to fulfill primarily safety, reliability, or security requirements. As mentioned in the previous subchapter, the permanently increasing numbers and capabilities of digital devices used in these applications along with their almost unlimited interconnectivity leads to the problem of "state space explosion". Strong efforts of basic and applied research are urgently required to develop adequate design, verification and validation methods, as well as testing strategies to guarantee these quality requirements.

The "Internet of Things"

The "Internet of things**"** is the vision that, besides human individuals, all kinds of objects, devices or goods of our everyday life ("things") can be connected through a future Internet. These "things" can receive, store, process, or emit data and information through communication with other "things", individuals, or services. This requires that many more "things" must have an Internet address – which will be

---

69 Kizito Ssamula Mukasa, Andreas Holzinger, Arthur I. Karshmer, "Intelligent User Interfaces for Ambient Assisted Living," Proceedings of the 13th International Conference on Intelligent User Interface, ISBN: 978-1-59593-987-6, 2008, http://portal.acm.org/citation.cfm?id=1378856; Fraunhofer IRB Verlag, ISBN 978-3-8167-7521-8, http://verlag.fraunhofer.de/PDF/English_Publications_2010.pdf.

70 P. Rashidi, D. J. Cook,"Keeping the Resident in the Loop: Adapting the Smart Home to the User," in *Systems, Man and Cybernetics, Part A:* Systems *and Humans, IEEE Transactions*, Sept. 2009, Vol. 39, Issue:5 at 949–959, http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=3468; The CASAS Smart Home Project, Washington State University, USA, http://ailab.eecs.wsu.edu/casas/.

feasible under IPv6 – and serve on itself or in subnets as physical source, destination or access point for communication, cooperation and computing.[71]

A step-wise implementation of this vision could realize the idea of "ubiquitous computing and communication" that Mark Weiser had expressed about 20 years ago.[72] A major characteristic of this vision is the development of technical objects towards "intelligent objects" which possess limited computing and reasoning capabilities, and which are connected through the Internet with cyberspace. An example for such an "intelligent object" could be an active sensor which receives information from other objects, processes that information and – based on its current status – reacts by sending response messages to other objects. This will enable communication between individuals and "things", but also between "things" themselves, offering completely new opportunities for applications, but also risks with respect to safety and IT security (privacy, authenticity, data security).

Current Threats

As mentioned before, the scale, complexity and openness of our digital networked world has reached a level where it is no surprise that abuse is growing quickly, and trends of future expansion of ICTs even increase the number and potential of threats if not considered carefully.

There are many reports, either by those interested in selling ICT security solutions, e.g. MacAfee,[73] Symantec,[74] Kaspersky,[75] or by others discussing more general security

---

71 *Internet of Things – An action plan for Europe*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf; "Appendix F: The Internet of Things (Background), Disruptive Technologies: Global Trends 2025, SRI Consulting Business Intelligence, www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf.

72 Mark Weiser, "The Computer for the Twenty-First Century," *Scientific American*, Sept.1991 at 94-110, www.cim.mcgill.ca/~jer/courses/hci/ref/weiser_reprint.pdf.

73 McAfee Security Advice Center, http://home.mcafee.com/advicecenter/.

74 "Internet Security Threat Report,"Symantec, www.symantec.com/business/theme.jsp?themeid=threatreport.

75 Kaspersky, www.kaspersky.co.uk/index.html.

issues or interested in security for their own IT systems and products.[76] Categories of cybercrime methods mostly addressed in these reports are:

1. **Malicious code or Malware**: software based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, crimeware, most rootkits, and other malicious and unwanted software.[77] Symantec reported an increase from 624 000 to 1 656 000 new malicious threats from 2007 to 2008.

2. **Spam** is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. The most frequently used form of spam is email-spam, or unsolicited emails with commercial content which are sent in large quantities. The low cost of sending creates a potential high value. Increasingly, however, spam is sent out with a criminal intent, containing malware or with the intent to deceive people to make payments, information releases, etc. (phishing).

   To hide the sender's address and enable high volume sending, criminals often use zombies or bots (others' computers which act as a remote slave under external control without the knowledge of the owner) or networks of zombies (also called botnets). It is estimated that in 2008 a total of 350 billion spam messages were sent, with 90 per cent through botnets. This is about 85 per cent of total messages worldwide.

3. **Phishing** websites and hosts are masquerading or spoofing the website or email addresses of trustworthy entities (e.g. banks) with the criminal intent to acquire sensitive information such as usernames, passwords or credit card details. Malware could be installed on a computer that will send the user to such a phishing website instead of the intended trustworthy site, or spam could be sent with spoofed addresses that invite the user to click on a link to a phishing site. Reports detected about 55 000 phishing hosts in 2008, an increase of 66 per cent over 2007.

4. **Bots and botnets** are being created using computers from many users without their knowledge. These are either directly used or "leased" for criminal use on the black market. Symantec found about 75 000 bot-infected computers per day and 15 197 distinct new bot command and control

---

76 "Security Tech Center," http://technet.microsoft.com/en-us/security/default.aspx; SANS, www.sans.org/.

77 *See* for this definition and further explanation: http://en.wikipedia.org/wiki/Malware.

servers. Underground economy servers provide a black market for stolen information (on credit cards, ID etc.) or selling/leasing of malware, or botnets.

Though it is generally reported that most attack origins are in the US, followed by Brazil and China, attacks can be launched by anybody at any time and even from remote locations. Although the Conficker attack, based on a zero-day vulnerability, is still fresh in our memory, it could be cautiously concluded that the number of serious zero-day vulnerabilities is decreasing due to the increased attention to the security of operating systems and applications by the large software companies.

Criminal intent focuses on the financial sector, which attracts more than 70 per cent of phishing, with ISPs in second place with only 11 per cent.

The *Whitebook: Emerging ICT Threats* by the FORWARD[78] consortium tried to explore emerging and future threats in a systematic fashion. They defined four axes along which future developments are anticipated or are currently unfolding: *new technologies*, *new applications*, *new business models*, and *new social dynamic*.

They identified 28 threats classified in eight categories:

1. *Networking:* threats related to the introduction and deployment of new network technologies, and to infrastructure services (routing, DNS) on the Internet.
2. *Hardware and virtualization:* threats due to new hardware and software developments related to virtualization and the Cloud.
3. *Weak devices:* threats that are introduced with new computing devices which are limited, both computationally and because of power constraints.
4. *Complexity:* threats that emerge due to the complexity and scale of future systems, which lead to unexpected and unintended dependency interactions, and security consequences.
5. *Data Manipulation:* threats that stem from the fact that people (and systems) store more data online, and this data is becoming increasingly valuable and sensitive.
6. *Attack infrastructures:* threats related to the fact that adversaries actively develop and deploy offensive platforms (such as botnets). They no longer perform hit-and-run attacks, but establish operational bases on the Internet for malicious campaigns.

78 "The FORWARD Emerging ICT Threats Whitebook," www.ict-forward.eu/whitebook/.

7. *Human factors:* threats due to insider attacks, especially in the context of outsourcing; and threats related to new social engineering attacks.
8. *Insufficient security requirements:* threats related to legacy and commercial-off-the-shelf systems that have not been built with sufficient protection and are now used and deployed in scenarios for which their protection mechanisms are inadequate.

This categorization allowed for prioritization of additional (research) efforts that would be needed to mitigate the threats, taking account of severity, expected likelihood and existing efforts. They concluded highest priority for threats related to: *parallelism, scale, underground economy support structures, mobile device malware* and *social networks.*

The current state of threats is clearly reason for alarm and needs urgent coordinated action at a global level by experts in a variety of disciplines, as well as politicians and diplomats. While some of those threats require primarily efforts towards evolved or improved security regulations, standards, techniques or tools, others urgently require basic scientific research efforts and solutions for practical implementation.

Conclusions

Future research and product developments of ICT will significantly influence individual, social and cultural behaviour worldwide in private and public life. The ongoing (r)evolution of digital systems, of the Internet, and of their services and applications are becoming basic resources for everyday life. This digital world offers lots of benefits and chances for humanity and for technical advances, as well as new ways to overcome some global problems like energy, or health care. Basic chances and benefits of future ICT technologies and applications are addressed in this chapter.

Despite these positive aspects, newer and greater problems are addressed which require more intensive basic research and appropriate solutions: the fundamental problem is the lack of design and analysis methods which are scientifically proven to master the enormous complexity of future interconnected digital systems, especially regarding safety, reliability, functionality and security (privacy, authenticity, data security). Developing solutions for this fundamental problem is one of the most important challenges for the computer science and web science research communities. Global distribution of an open “hard problems list”, as the one prepared by the World Federation of Scientists, together with efficient countermeasures – if available – could be a very useful step in this regard.

But this “mastering gap” not only refers to current design and production techniques. Consequences of human errors, technical faults, failures, or misuse and manipulation

always have to be taken into account, and countermeasures have to be developed and applied – the latter as far as possible regarding given constraints.

In addition, adequate measures are missing to make users, consumers and institutions aware of major problems, risks, or even threats using ICT resources. Media professionals should be involved in developing information materials on IT security issues to address different audiences. As discussed in chapter II, modern societies depend on ICTs and an evolving Internet. Therefore, consequences of future technological developments towards a digitized world have to be carefully analysed and communicated in order to build trust.

4.2 Government Internet Censorship: Cyber Repression

By Henning Wegener

Free expression of opinion and free access to information are at the very centre of a functioning Information Society and are essential ingredients of cyber stability and cyber peace as defined in chapter VI in "A Concept of Cyber peace" by the same author. Threats to their exercise undercut or deny key benefits of the Internet, and are therefore to be ranked among the major current threats in cyberspace.[79]

Freedom of opinion and free access to information have throughout history been key elements in building civilized societies. They are an indispensable part of human rights and civil liberties, and are consequently centrepieces of almost all modern constitutions. Indeed, the freedom of the individual to acquire information, hold and communicate opinions could serve as a yardstick of human progress. On the other side, the definition of the limits which this principal freedom must undergo for reasons of public security, decency and *ordre public* have always been an intrinsic element of internal political debate, a permanent and necessary effort in the quest for reconciling and optimizing both individual liberty and public interest.

Government censorship in terms of systematically overstepping these limits and exercising close control over public opinion and exchange of views, mainly in respect of printed material, is a painful but recurrent part of human history, and has again and again triggered battles for the freedom of the mind.

In the Internet age, this basic constellation has not changed, but its relevance and the form it takes indeed has. Digital technologies have catapulted the opportunities for access to information and communication into a new dimension; this is the essence of the Information Society that is now upon us. As in every other aspect, the Internet

---

79 The World Federation of Scientists has previously dealt with this problem in its submission to the World Summit on the Information Society (WSIS) at its Tunis phase 2005, "Information Security in the Context of the Digital Divide", specifically in Recommendation 5 contained therein, "Denial of information access through Internet filtering", p. 12, and Explanatory Comments p. 24 -30, www.itu.int/wsis/docs.2/tunis/contributions/co1,pdf, , and www.unbiw.de/infosecur. *See also*, with a similar thrust as the present chapter, Henning Wegener "Cyber Repression: Framing the Problem. Assessing the State of Debate and Thinking of Counter-Strategies," in *Rights and Responsibilities in Cyberspace. Balancing the Need for Security and Liberty*, 2010, EastWest Institute and World Federation of Scientists, www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

enlarges amplitudes, confounds the measures of quantity and quality, negates distance and time, and creates ambivalent new phenomena.

For the Internet does not only increase information and its accessibility on an exponential scale, it also increases the potential to intervene in the underlying technical processes and manipulate digital contents. Digital technology allows for filter software which can block any area of information, through the entire Internet or only relating to certain servers, and it allows governments to introduce Government censorship, including on a massive scale. The issue of freedom of opinion and information as a human right must thus be considered afresh: the Internet is rapidly becoming the new battleground in the struggle for human rights and freedom of opinion.

The principal techniques available to censoring governments are IP blocking, DNS filtering and redirection, URL filtering through scanning for target keywords, or packet filtering, which is terminating TCP packet transmission once controversial keywords are detected. One characteristic is that current filter software reacts only mechanically to the occurrence of certain words or phrases, and thus often overshoots the target ("over-blocking").

The number of industrial suppliers of filter software employing these and other techniques is legion. They include most of the big names of information technology, but also specialized companies. There are several webpages dedicated to evaluating comparatively and rating such software offers as to their efficiency, while other pages operated by the advocates of total freedom of expression in the Internet criticize the very emergence of this technology.

Filtering technology has to be viewed together with the options for circumvention. The same sophistication that has marked the development of filters also characterizes the technologies designed to avoid, circumvent or damage the filters. Total censorship of information on the Internet is very difficult or even impossible to achieve due to the underlying distributed technology of the Net. There are thus a number of resources and solutions that allow users to bypass Internet censorship. Most of them rely on gaining access to an Internet connection that is not subject to filtering, often in a different jurisdiction not exposed to the same censorship laws. The obvious challenge to the practitioners of Government Internet censorship is that so long as there is *one* publicly accessible system in the world without censorship, it will still be possible to have access to censored material. The techniques available for this surreptitious access include the use of proxy servers, the establishment of virtual private networks, and the downloading of open source software that allows for anonymous surfing, chatting and file transfers (examples are Psiphon, I2P, Tor).

Content filtering, to be sure, also serves an important societal protection function. Blocking pages of child pornography, incitation to violence, racial hatred and crime in general would appear legitimate to anyone, and the same holds true for the increasing utilization of the Internet by national and international terrorism. Content that may not be disseminated legally *outside* the Internet needs to be susceptible to legal sanctions and interdiction also *within* the Net. In this regard, the filter software industry fulfils a legitimate need.

But here an important distinction has to be made.

Whatever the efficiency of filters, and thus the censorship effect, and whatever the commercial interests involved, decisive is the fact that in the "free" societies, mainly – but by no means exclusively – of the so-called Western democracies with their high degree of value consensus, the restrictions on freedom of expression and access to information are clearly regulated by law, their scope is governed by the rule of adequacy and proportionality, and they can be evaluated in publicly accessible legal review procedures. The existence of a clear legal framework and the availability of independent legal control are, indeed, the decisive criteria for distinguishing legitimate content control from illegitimate censorship; they also provide the instrument for accommodating differences in cultural values and definitions of privacy. Content offensive to culture, religion, morals and other deep-seated collective beliefs within certain countries should not be exempt from control under the banner of absolute Internet freedom, and those who rightfully denounce government political censorship should be careful to take sides on such issues.

As Government Internet filtering, the limits to the restriction of freedom of expression that should be observed, the balances that should be struck, and the role of the IT industry in providing the technical underpinnings for Internet control all touch on delicate issues of national sovereignty, this article refrains from placing blame or responsibility on any individual government; in fact, no country is mentioned by name. Equally, no IT hardware, software or service provider is named. Indeed, the purpose of the article is to frame the problem and assess the state of debate, not to rush to conclusions. In the same spirit of restraint, citations of webpages or articles are provided for reference only, and do not imply that the article identifies with, or endorses their contents.

Given the frontier-less nature of the Internet, national rules are not sufficient to administer Internet freedom. Thus, the European Union has put in place since 1999 an incipient EU-wide regime to regulate admissible inroads to Internet contents and relevant procedures ("Safer Internet Programme"). It relies mainly on the principle of self-regulation by the Internet industry and search machines to exclude illegal or

damaging contents and to ensure conformity with national legislation. In some areas, this self-regulation functions satisfactorily, even though complementary legislation may occasionally be required.

Globally speaking, international legal standards are set in particular by the two great human rights treaties from the early years of the United Nations – the *Universal Declaration of Human Rights (1948)* and the *International Covenant on Political and Civil Rights* of 1966. Practically all nations have signed and ratified these pacts which are now considered international customary law, thus binding also for non-signatory States. By coincidence, in both documents it is in Art. 19 that the principle of freedom of expression and opinion is recognized, which includes the right of anybody to receive and impart information of all types, regardless of frontiers and through any chosen medium. There is no doubt that this also includes the reception of information through the Internet and the right of access to it (just as much as the right *not* to be accessed), and thus the World Summit on the Information Society (WSIS, 2003 and 2005) has solemnly confirmed these principles as central to, and an indispensable pillar of, the information society, specifically in the *Geneva Declaration of Principles* (principles 4, 5 and 55). It is worth noting that the WSIS text emphasizes the liberty aspect, deemphasizing the caveats added in the International Covenant.

What in the "free" societies boils down to a problem of an – admittedly difficult – permanent political balance between freedom and State intervention under clear legal criteria, in many other States thus becomes a problem of human rights and of the quality of a global information order. Internet censorship by governments via filter technologies without legal constraints, and with grave and incisive consequences for the individual seeking and imparting information, constitutes a human rights violation of highly relevant dimension. A problematical component of this development is that Western technology companies not only provide their filtering technology to the censorship-prone governments, but also collaborate in their use, thus establishing effective and efficient censorship systems. This phenomenon is central to the present analysis, which also aims to suggest possibilities of international action against these practices. As Jo Glanville, editor of "Index on Censorship",[80] has remarked: "Censorship, for the first time in its history, is now a commercial enterprise".[81]

---

80 Index on Censorship is a prominent British organisation promoting freedom of expression, www.indexoncensorship.org.

81 Jo Glanville, "The big business of net censorship," *The Guardian*, 17 Nov. 2008, www.guardian.co.uk/commentisfree/2008/nov/17/censorship-internet.

This is written at a time when a critical growth process can be observed both in the number of governments which practice Internet censorship, mostly to the detriment of political rights and freedoms, and the proficiency of filtering techniques.

The state and development of Government Internet censorship is monitored by many private institutions, including the trail-blazing OpenNet Initiative, Reporters Without Borders and, often using the same or similar data and categorizations, the Internet Censorship Report.[82]

These sources unanimously observe a growth process of censorship of staggering proportions. Based on their country lists and figures they conclude that at present 1.72 billion people are affected by Internet censorship. This would amount to 25.3 per cent of the current world population.

The list of States given to these practices is long – at least 25, probably more than 30 – governments seriously deprive their citizens of the possibility of access to the full range of information available online. The Internet provides several lists by organizations that monitor these countries. The Opennet Initiative categorizes them as Pervasive, Substantial, Nominal and Indirect, and also maintains a Watchlist category. Reporters Without Borders has a top list of 13 "Enemies of the Internet". Most of the countries monitored concentrate their intervention on banning political content – freedom, democracy, free elections, legal remedies, reports about sensitive political events – which their own system of government does not allow, but many go beyond. Some governments concentrate their restrictions on moral themes, their inherited moral and cultural order. The intensity and thoroughness of control varies. There are some countries in which the censor blocks pages, but then deviates the call to an explanatory page, providing access if special "legitimate" interest in the information is shown, thus affording at least some degree of transparency. In other countries, censorship is practiced sporadically and ineffectively, and sanctions are not applied in case of breach of blockage.

---

82 OpenNet Initiative, www.opennet.net. The project employs an international network of investigators to determine the extent and nature of government-run Internet filtering programs. Participating academic institutions include the Centre for International Studies at the University of Toronto's Munk School of Global Affairs, the Berkman Center for Internet & Society at Harvard Law School, the Oxford Internet Institute at the University of Oxford, and the SecDev Group, which took over from the Advanced Network Research Group at the University of Cambridge's Cambridge Security Programme. See also www.chillingeffects.org with an even larger group of supporting academic institutions which "monitors the legal climate for Internet activity."

As a rule, however, government censorship is exercised without limits and over a broad segment of human knowledge, without any explanation or justification of the underlying rationale, even by some otherwise quite respectable countries: the farther away from Western-style democracy a country, the higher the incidence of censorship through Internet filtering. Some States push the tutoring of their population through Internet censorship to particular extremes: Internet users caught in accessing prohibited pages are punishable, and in some countries persecuted by an aggressive cyber police. The number of users in jail, as far as is known, is alarming from any point of view. Some international IT companies providing the software have to live with the suspicion that they actively aid and abet such measures of prosecution, and thus contribute to the resulting human suffering.

The consequences of comprehensive censorship are grave, and cannot be overestimated. Citizens are not only curtailed in their rights under international law, they are cut off from important benefits of the information age, they receive a skewed view of world reality, their participation in enriching global communication processes is diminished. Massive Internet filtering can alter the collective state of mind of a nation. One must also take into account the *dual* negative effect of this censorship: citizens are deprived of information and an unencumbered world view, but the censorship is also a tool of their political repression, curtailing freedom of action.

This state of affairs, and the worsening record of Internet censorship acutely call for action. The EU for one has recognized this and taken action. It does not accept that repressive governments are assisted by IT technology companies in solidifying their mental dictatorships. We also owe it to the EU to have coined the highly appropriate term “cyber repression” to designate these practices.

The EU is not alone. The international Internet lobby which fights for the freedom of information and the integrity of the Internet worldwide, is active and vigilant, even beyond the many prominent institutions already mentioned which monitor the development of cyber repression and denounce it publicly.

Given the ability of experienced Internet users to avoid or circumvent filters, many international defenders of Internet freedom have also engaged in providing the citizens in censured countries with the corresponding counter-software such as described further above. These anti-filter technologies also have developed into a veritable industry that helps to diminish the effectiveness of government censorship, without being able to eliminate it entirely. The Open Net Initiative, like others, is active in this field supplying systems of particular effectiveness (like Psiphon), designed to allow a regular home computer to act as a personal encrypted proxy server and thus to jump obligatory “firewalls” introduced by the government and to navigate freely in

the global Net. However, the application of this device and other similar ones is being actively fought by certain filter providers. This again demonstrates the problematic nature of commercial activities of multinational industries which – intentionally or as unwanted collateral damage – in effect facilitate or assist cyber repression. Obviously one has to add that countries advanced in digital technologies are able to develop the filters domestically, and many are already doing so, which would allow foreign software providers off the hook.

As has been underlined before, this article does not purport to provide a detailed country-by-country analysis, given also that the Internet provides ample information to that effect. But even the brief summary description here given, and the nascent public discussion raise the question how the obvious need for action can be met, and what the international community can do to counteract cyber repression as a continued violation of international law.

The legal and political problems involved in defining the limits of internationally acceptable Internet filtering and possible sanctions are evident and they are huge. Questions of national jurisdiction and sovereignty, the near impossibility of developing broadly valid borderlines between civil liberties and overriding public interests, questions of choice of law and means of enforcement, and the larger issue of Internet governance, *inter alia*, render an attempt at international codification unfeasible and probably futile. There is also the question of cultural diversity and the respect others owe it. The definition of cultural and religious *ordre public* cannot be uniform for all countries, although we can legitimately assume a universal body of shared basic convictions, and although the Universal Declaration and Covenants must be considered universally binding. As mostly in international law, there are no easy definitions, and no rapidly effective sanctions.

Any reform of global Internet filtering must thus be looked upon in *terms of process* and of *strategies over time.* One should think in terms of procedures that arouse world consciousness, generate public awareness and pressure, and – for the governments affected – a public opinion challenge and motive to provide detailed justifications.

An important responsibility lies with national governments, industry, and the institutions of civil society with their opinion-forming potential. Governments can promote the development and availability of anti-filter technologies, can submit the export of filter technologies to appropriate export controls, and use national diplomatic means to exercise pressure on censuring governments, in the interest of transparency, to lay open and justify their restrictive policies.

The IT industry – software producers, and companies providing ISP services and their associations – bears obvious responsibilities and should proceed to adopt codes of

conduct which would exclude the use of their technologies for political censorship. While realistically one cannot ask companies to entirely set aside their profit interests, and while it would be foolish to shift the principal blame for government censorship to industry, voluntary collective action by companies also has a reputational aspect and will enhance positive images. Self-regulation policy, providing clear common standards, has given good results in the EU, and can also strengthen the power of resistance of individual companies to withstand the pressure of censorship-prone governments eager to do business with them. As an example, the Global Network Initiative, a voluntary effort by USA technological companies, prescribes such standards ("Governance Charter"), reacts to government requests for censorship and promotes Internet freedom.[83]

Academic institutions and human rights organizations which tirelessly denounce cyber repression – several of them are named above, are now increasingly encouraged and supported by governments that embrace their cause. But given the trans-frontier and international nature of the Internet, and the global human rights relevance of cyber repression, the most important task may be to put the issue in a major new way on the agenda of international organizations.

A first step could consist in reaching a broader international understanding on the development and technical underpinning of current Internet filtering and in creating an international monitoring mechanism.

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

Which international organization or body could be put to the service of this struggle?

In the first place, one could think of the Internet Governance Forum (IGF), created in 2006 in pursuance of decisions by the WSIS ("Tunis Agenda"). The restrictions which political Internet censorship place on the functioning and management of the Net are of obvious relevance for the Assignment of the Forum, and could easily be subsumed under its mandate (art. 72 a), b), e) and k) of the Tunis Agenda), even though the problem of cyber repression is not literally mentioned in these texts. Regretfully, the IGF in the five years of its existence has limited itself to admittedly rich and meaningful discussions, including on the freedom of the Internet; but operational activities have not been initiated. The establishment of a monitoring procedure where filter practices

---

83 Global Network Initiative, www.globalnetworkinitiative.org.

could be followed, analysed and critically evaluated would, under the terms of reference of the Forum if its mandate is extended as appears likely, be possible and desirable.[84] (The annual WSIS forum, by contrast, is an open-ended discussion forum without an operational assignment and would be less appropriate for this purpose.)

UNESCO proudly proclaims itself, under its foundational act, the unique international guardian of freedom of information, and has received from the WSIS clear tasks under the headings "Access to Information and Knowledge" and "Ethical Dimension of the Internet". UNESCO has adopted Declarations and Recommendations that commit member States and international organizations to free and unencumbered access to the Internet,[85] and its Director-General is ceaseless in publicly denouncing violations of the freedom of information and the press. Nothing would be more logical than to initiate in the fulfilment of these tasks a dialogue and, as an outcome, a periodical examination of censorship practices.

As we are dealing with human rights and the two basic international covenants setting out the obligations of States under them, the principal venue for international action should be the special human rights organizations within the United Nations, the Human Rights Council established in 2006, and the special body for dealing with violations of the *International Covenant on Political and Civil Rights.* The Human Rights Council, with its broad mandate, would be entitled to put in place a formal complaint procedure available to all UN member governments. One possibility would also be to insert the topic of Internet freedom and censorship obligatorily in the Universal

---

84 At least the IGF has shown that the censorship issue is not alien to the purview of its work. During the current debate on a continuation of the Forum's work and a possible amplification of its mandate, proposals have been made for more dialogue on freedom of expression, and more attention to the development and human rights dimension of International Governance. *See* UN General Assembly document A/65/78 (E/2010/68) of 7 May 2010.

85 "Declaration on Fundamental Principles concerning the Contribution of the Mass Media to Strengthening Peace and International Understanding, to the Promotion of Human Rights and to Countering Racialism, Apartheid and Incitement to War," United Nations Educational, Scientific, and Cultural Organization, 28 Nov. 1978, http://portal.unesco.org/en/ev.php-URL_ID=13176&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html; "Recommendations concerning the Promotion of Use of Multilingualism and Universal Access to Cyberspace," United Nations Educational, Scientific, and Cultural Organization, 15 Oct. 2003, http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html (advocating "universal access to the Internet as an instrument for promoting the realization of the human rights as defined in Art. 19 and 27 of the Universal Declaration of Human Rights").

Periodic Review process where country human rights records undergo a peer review. Whatever procedural form is chosen, collective highlighting of human rights abuses in this sphere could generate welcome pressure and argumentative necessities for governments suspected of illegality. Within the complaint procedure the dubious role of the international IT industry in instrumentalizing cyber repression could also be adequately illuminated. As in the HRC, the periodic country reviews in the UN Human Rights Committee could also include Internet freedom.

However deficient such merely procedural devices may be, a highly visible comply-or-explain regime, resulting eventually in public pressure and public opprobrium, could indeed pave the way for more global awareness of the problem, and for an eventual streamlining of behaviour in the digital world.

5 Cyber Conflict & Geo-Cyber Stability

5.1 Cyber Conflict

By Giancarlo A. Barletta,[86] William A. Barletta,[87] Vitali N. Tsygichko[88]

Introduction: The Nature of the Challenge

Information warfare is as old as human conflict. Few of the motives have changed; they include undermining the confidence of the adversary, impairing and confounding the adversary's lines of communication and creating illusions concerning the nature of and setting for conflict. These motivations have remained. What is very new in the 21st century, a time of pervasive electronic information infrastructures with ever-expanding, high bandwidth digital links is: a) the virulence and frequency of information attacks that can disrupt the social fabric of the target country; b) a far-reaching potential to effect extensive physical damage; c) the contagious capability and capacity for sustained information attacks open to non-governmental and even private actors that can now participate in asymmetric warfare; and d) the development of a pervasive underlying state of perpetual low-level conflict – what might be called a cyber cold war. The intensive introduction of new information technologies has considerably increased the combat capabilities of conventional armaments and other military technology. For this reason, militaries now consider information and communication technologies (ICTs) to be both weapon and target and view cyberspace as a domain for warfare similar to air, space, land and sea.[89]

Over the past two decades, industrialized nations have deployed pervasive networks of major economic, physical and social assets connected via ICTs to advance their

---

86 Global Cyber Risk, LLC; Washington, DC, USA.

87 Massachusetts Institute of Technology, Cambridge, MA, USA.

88 Institute for Systems Analysis, Russian Academy of Sciences, Moscow, Russia.

89 For example, "The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests – to fly, fight, and win in Air, Space, and Cyberspace." "Air Force Strategy: Sovereign Options for Securing Global Stability and Prosperity," 26 Mar. 2008, Office of the Secretary of the Air Force, www.stormingmedia.us/98/9868/A986884.html. The US perspective is further elaborated in *Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service (CRS) Report, RL31787, 14 Sept. 2006, www.fas.org/irp/crs/RL31787.pdf (hereinafter "CRS Report").

standard of living, economic prosperity, international influence and power. Likewise developing nations see information technology as an economic fast track to full participation in the global economy. Smart devices for industry (containing both sensors and micro-processors) abound, as do consumer devices with microprocessors and wireless (or cellular) capability such as cellphones, PDAs and electronic notepads. Extensive communications networks permit the intensive application of information resources to facilitate commerce, provide services, monitor the environment and address complex societal problems. All these devices are developing rapidly with the capability to communicate with other devices anywhere on the globe.

As a former U.S. military general notes, these same ICTs that connect major economic, physical and social assets have been adopted and adapted by militaries and quasi-military movements, contributing to a revolution in military affairs that is changing the way warfare is planned, organized and conducted. This "revolution" encompasses developments in the ability to conduct intelligence, surveillance, and reconnaissance; to command and control forces and their operations; to optimize logistical movements; to enable precision navigation and the employment of "smart" weapons. Very significantly, it also allows for the use of the "network" as a medium from which, through which and in which to conduct military operations.[90]

Information technologies invite and facilitate new causal relationships throughout societies with a natural potential to enhance economic growth, to advance human rights and to expose government repression. National command authorities enjoy greatly facilitated top-down communication but, more importantly, with respect to expanding human rights and economic well-being, the streams of bottom-up and horizontal information flows have expanded to great rivers. Modern information societies continually augment both the number and the attributes of information nodes (where information is generated and consumed) and the number and bandwidth of links. Moreover, an increasing percentage of both nodes and links carry autonomic sensors of their operational status.

Such highly non-linear connectivity simultaneously increases both the resilience of the information network and risks and consequences of debilitating attacks on the nodes and backbone links, and the difficulties of anticipating the consequences of network failures. The rapid development of ICTs and the consequent evolution of the global information society have the potential to breed a wide range of negative geopolitical

---

90 Gen. John Casciano, "Threat Considerations and the Law of Armed Conflict," Aug. 2005 (on file with WFS Information Security PMP).

implications: a faster global polarization between wealthy and poor nations, an ever-wider technological gap between highly industrialized and developing countries, leaving an increasing number of economically marginalized countries along the roadside of evolution of civilization – a major breeding ground of political instability and conflicts. Consequently as the complexity of information networks evolves organically, the potential of information warfare evolves toward putting ever-greater societal value at risk.

Public Proscription of Cyber Attacks vs. Government-led Cyberwar

Attacks against computer networks, systems and digital data have led to the enactment of cybercrime laws in many countries. Although most industrialized countries have some sort of cybercrime law, significant variances in defining what constitutes a cybercrime, in detecting and identifying criminal behaviour in cyberspace and in the applicable substantive and procedural provisions have significantly hindered international cooperation in providing assistance in cybercriminal investigations. The Council of Europe (CoE) Convention on Cybercrime was developed as a multilateral agreement that was intended to initiate the harmonization of global cybercrime laws. Reality has fallen short of expectations, however; only 26 countries had ratified the CoE convention by mid-2010, nearly nine years after it was opened for signature. The ITU Toolkit for Cybercrime Legislation has been developed as an alternate path with more flexibility; it provides sample legislative language that is harmonized with the CoE convention and cybercrime laws in industrialized nations and may be used by countries around the world in drafting or amending their own cybercrime laws.

Other laws pertaining to certain types of cyber activities include those protecting physical systems and equipment of communications providers, statutes prohibiting acts of economic espionage, intellectual property laws, etc. In all, these laws are intended to provide a legal proscription to cyber attacks of various sorts against all types of infrastructure, systems and data.

The broad range of possibilities grows wider each day with the advent of more powerful and more pervasive information technologies. Little wonder that nations have a strong motivation to codify conduct in cyberspace regardless of their own behaviour toward other nations. As information technologies can readily hop international borders, criminals need never physically enter the state in which the victim is located. Consequently, the incentives for cooperation among nation states should be large, especially as state information resources form an attractive target for criminal behaviour. Indeed, cooperation both in promoting fruitful collaboration in and through information networks and in preventing or at least deterring misconduct in cyberspace has become the concern of inherently international bodies such as ITU.

Because governments increasingly rely on the Internet to facilitate the distribution of information and services to their citizens, the information society presents a tempting target to miscreants, be they criminals, sub-national terrorist groups or hostile nation-states. The attack[91] on the national information infrastructure of Estonia in April, 2007 clearly demonstrates both the predicted vulnerability of an e-government and the absence of factors that would deter an attacker. Many experts have claimed that the technical sophistication of the attack exceeded that of previous known incidents. While some go so far as to say that the knowledge or collusion of a national entity was required, several US experts have discounted such speculation. One should note, however, that the Estonian episode was not accompanied by political or monetary demands or by manifestos from the putative leaders of the attack,[92] making criminality without political motivations unlikely.

Other examples of more sustained and more extensive cyber attacks are offered by the GhostNet[93] and Aurora attacks of 2009. One aspect of the attacks was focused on Google servers as part of an apparently concerted political and corporate espionage effort that "exploited security flaws in e-mail attachments to sneak into the networks

---

91 The attack has been widely reported in the international press. For example *see,* Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* 17 May 2007, www.guardian.co.uk/world/2007/may/17/topstories3.russia.

92 By early June a leader of the pro-Putin Russian youth group, Nashi, had claimed credit for the attack. www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html . The veracity of the claim is unknown.

93 *Tracking GhostNet: Investigation of a Cyber Espionage Network,* Information Warfare Monitor, 1 Sept. 2009, www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/. "The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information…. But attributing all Chinese malware to deliberate or targeted intelligence gathering operations by the Chinese state is wrong and misleading. Numbers can tell a different story. China is presently the world's largest Internet population. The sheer number of young digital natives online can more than account for the increase in Chinese malware. With more creative people using computers, it's expected that China (and Chinese individuals) will account for a larger proportion of cybercrime."

of major financial, defence and technology companies and research institutions in the United States".[94]

As the Estonian incident illustrates, intense and sustained cyber attacks may constitute *de facto* a direct and substantial assault on civil and state entities at a level that rises above mere criminality. The characteristics of such attacks may include: a) serious physical damage to critical facilities; b) widespread injuries or loss of life; c) disarray in financial institutions; and d) interruption of the functionality of critical infrastructures. The coordination or continuity of such attacks for extended periods is likely to compound the severity of the consequences. In such circumstances, whether the identities or motives of the attacker are known, nation states might regard[95] an extensive cyber attack as an act of terrorism or the functional equivalent of an armed attack that justifies special consideration and special treatment to redress.

At the very least, the demonstrated potential for large-scale disruption of an information society calls for a culture of mutual cooperation across national lines. In the Estonian example, the first wave of disruptions of government sites set in motion response plans that anticipated a wave of attacks on financial services such as online banking. In fact, within a few days, "[p]rivate sector banking and online media were also heavily targeted and the attacks affected the functioning of the rest of the network infrastructure in Estonia."[96] During that same period, the countermeasures, undertaken with the cooperation of ISPs worldwide, were to expand blocking of traffic from specified groups of IP addresses and to wall off the Estonian banking system from all international traffic. It is noteworthy that the network of resources required to ameliorate the consequence of the cyber attacks must have exceeded by a large factor the resources used to launch the attacks.

The considerable asymmetry between offence and defence in cyberspace has not gone unnoticed. Short of such large scale attacks, military and intelligence agencies of the United States and other nation states (Russia, China, India, Pakistan, Iran) already

---

94 Ariana Eunjung Cha and Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say," *The Washington Post*, 14 Jan. 2010, www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

95 For example, in 2009 former US Director of National Intelligence, Mike McConnell, categorized cyber-weapons as a weapon of mass destruction (or potentially so). CRS Report at 3.

96 "ENISA commenting on massive cyber attacks in Estonia," ENISA press release, 24 May 2007, www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia.

"reconnoiter and probe to identify exploitable digital network[s] by weaknesses among potential adversaries." The decision makers in these countries act as if the age of cyber conflict is now. In fact, it is countries like the US that have the asymmetric capability and capacity to launch or sponsor cyber attacks (especially as covert operations) upon countries less able to respond in kind. Moreover, the authorities in these and other countries are well aware that the large offence-defence asymmetry when coupled with the near anonymity of a determined attacker gives rise to the possibility of employing either directly or indirectly small "armies" of cyber mercenaries or "illegal combatants" who provide national authorities with an aura of plausible deniability.

In practice, the damage potential of a given attack can vary greatly depending on the degree of preparedness of the society and the built-in security of the infrastructure under attack. From the point of view of the political or military decision maker, the "important issue in countering any form of cyber attack is to quickly discern the type of attack and the adversary and then to respond appropriately. Currently, tracking down computer intrusions is a law enforcement function. ... The traditional war fighting military is prohibited from executing this mission domestically … [therefore] domestic law enforcement has a critical role in national security and national defence."[97] It follows that nation-states in both their military and law enforcement agencies require powerful digital forensic tools, an appropriate legal structure to use them, credible approaches to preserving the integrity of evidence and penalties for transgressors that have real deterrent value. As these tools have strong "dual use" potential, those nations which acquire the strongest and most flexible defensive and forensic capabilities will, *a fortiori*, have in hand considerable offensive and cyber espionage capabilities. While dual use potential and offence–defence asymmetry are also present in the realm of physical weaponry, the likelihood of kinetic attacks is suppressed (though not eliminated) by the concepts of deterrence and by the relative ease of attribution of the source of the attack.

The Interplay of Information and Kinetic Conflict

The intensive introduction of new information technologies both reinforces and increases combat capabilities of conventional armaments and military technology.

---

97 Bonnie N. Adkins, "The Spectrum Of Cyber Conflict: From Hacking to Information Warfare: What Is Law Enforcement's Role?" Air Command and Staff College, Maxwell Air Force Base, AU/ACSC/003/2001-04, Apr. 2001, http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA406949.

Information technologies enable qualitative changes in military and reconnaissance and communications. They greatly increase the speed of processing huge arrays of data and making complex operational decisions, thereby making it possible to transition to radically new methods of control of troops and armaments at all levels – from strategic to tactical.

New information technologies sharply increase combat capacities of electronic warfare facilities and create a new type of arms, notably, information weapons designed for damaging an adversary's military and civilian information infrastructure by piercing its computer networks.

For the military, the information and technological revolution sharply increases the combat capabilities of troops, not only changing the forms and methods of different scales of warfare but also changing the traditional paradigm of military struggle and conflict escalation. According to US experts, selectively targeting information weapons on an adversary's critical military and civilian information infrastructure could terminate a conflict prior to the beginning of kinetic combat operations of the parties, as an escalation of information attack results in disaster. The possession of information weapons provides an overwhelming advantage over nations lacking them. If not today then in the near future, the information and political variables of the confrontation of powers will dominate the nuclear ones. In contrast, all countries, especially highly developed ones, are vulnerable to information weapons. Information weapons, just like nuclear ones, can serve as both a factor of political pressure and deterrence.

Information warfare is not a virtual reality of computer games but a quite tangible tool of gaining victory in a military or political conflict. Without doubt, information weapons becoming a major component of the military potential of a nation, and many countries, in particular, the USA and China, are persistently and actively preparing for waging information wars.

The Nature of Information Weapons

A conceptual problem of formulating an information security paradigm is defining and identifying "information weapons". What are the distinctive features of information weapons? What (if any) level of cyber conflict should be treated as armed conflict? The absence of any international consensus regarding these questions impedes launching constructive negotiations on global information security. One approach to defining the "information weapons" concept rests on their ability to affect military and

civil information infrastructure.[98] A drawback of this approach is that any type of weapon, including conventional ones, could then be called an information weapon, if it is capable of damaging components of information infrastructure. For example, does it matter what device has rendered the control system of a municipal economy non-operational – be that a program code, an intensive electronic pulse or a direct hit of a conventional explosive? A second approach might be to designate as information weapons all means of destruction that use ICTs.

What must be avoided in confronting the issue of cyber conflict is lowering the barrier to war by adopting definitions that include activities that are frequently carried on during peacetime. What are the distinctive features of information weapons? What level of cyber conflict should be treated as armed conflict? It would be unwise and dangerous for international stability to treat conflicts that have no clear threats to human lives or societal freedom as an "armed conflict". Moreover, as practically all sophisticated weapons systems make use of ICTs, it is extremely difficult, if not impossible, to single out information weapons from the entire range of armaments. As information warfare is a persistent phenomenon in the history of human conflict, a crisp definition is especially difficult, in the presence of several levels of conceptual complexity. For example, how should one classify providing deliberately wrong information? What about espionage, or interception of information flows? One's perspective concerning such activities would be strongly influenced if they were executed during kinetic war.

The important operational characteristics of information weapons are 1) their relatively low cost and accessibility; 2) the possibility of latent development, accumulation and introduction; and 3) their intrinsic extra-territoriality and anonymity of impact. These features enable the uncontrolled spreading of information weapons and make their possession by aggressive regimes a dangerous global issue. The consequent threat to international peace and stability calls for the global community to control the threat to national and global information security infrastructures through practical steps towards the neutralization of cyberthreats. Being a part of the

---

98 For example, "Any capability, device, or combination of capabilities and techniques, which if used for its intended purpose, is likely to impair the integrity or availability of data, a program, or information located on a computer or information processing system." Graham H. Todd, "Armed Attack In Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition," *Air Force Law Review,* Vol. 64, 2009 at 65 – 102, http://lawlib.wlu.edu/CLJC/index.aspx?mainid=418&issuedate=2010-03-23&homepage=no.

infrastructure of modern society, ICTs are therefore part of a nation's set of instruments to fight its enemies.

Many countries are taking measures to counter threats to information security; yet the efficiency of even tough measures is reduced by the transnational nature of the threat and the anonymity of transgressors. In such circumstances no nation can be safe if attempting to fight back information threats by itself, alone. Only creation of an international information security regime and the concerted efforts of its participants can ameliorate the proliferation of information weapons and reduce the threats of information war, information terrorism and cybercrime.

At a minimum, software designed exclusively for destroying information infrastructure (different viruses, bookmarks, etc.) can be unambiguously referred to as information weapons. The bulk of sophisticated means of armed struggle, making use of ICTs, are multi-use, i.e., designed not only for destroying information infrastructures but for other combat tasks. The nations possessing such sophisticated weapons systems, means of reconnaissance, communication, navigation and control based on a wide-scale application of ICTs boast a decisive military advantage; hence, it is doubtful that they will ever enter into agreements limiting their strategic advantages.

Therefore, the very issue of banning or limiting production, proliferation and application of information weapons is likely to be limited to single-purpose weapons designed only for hitting information infrastructure components, e.g. weapons based on program codes, i.e., various viruses and means of their delivery. Unfortunately, the overwhelming majority of modern ICTs, which can be used for military, terrorist and criminal ends, are developed in civilian industries; thus, the control over their development and proliferation is very difficult.

The threat posed by instruments for cyber conflict and information warfare is real for all, especially for advanced nations, where the complex information infrastructure determines all of their vital activities.[99] Only the concerted efforts of the international community to secure critical national information infrastructures are likely to ameliorate the threat of the malicious use of information technology. Consensus concerning this class of information systems will enable more effective deterrence as

---

99 The U.S. military's decision not to launch a cyber attack on Iraqi financial systems is discussed in *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, RL31787, 19 July 2004 at 5-6, www.fas.org/irp/crs/RL31787.pdf. This CRS report also lays out the U.S. military's framework for addressing cyberwarfare and explains where cyberwarfare fits within the military's long-running strategy and programs on information warfare.

well as more efficient protective measures, including the right to use retaliatory actions in the event of information operations against them that have serious, unacceptable direct effects. Even here extreme caution is in order. Initiating kinetic war is not justifiable by just any aggressive information act; it would be unwise to give governments arguments to decide to do so on their own.

Limiting of Cyber Conflict

The potentially gross asymmetry between offensive and defensive information technologies leads to the condition in which end-users can wage personal "cyberwars" against a society's critical information infrastructure with nearly the same strength as nation states. Consequently the legal and political regime of deterring and limiting cyber conflict between nations will de facto be connected with the legal and procedural frameworks for deterring and handling cyberterrorism and cybercrime.

In the realm of the information society, the concept of deterrence through civil and criminal penalties may be operable at the level of criminality or "hacktivism"[100] if a suitable network of international homogeneity in criminal codes can be established. Unfortunately, at the level of cyber attacks by nation states, the concepts of deterrence developed during the Cold War may have little value, as a counterattack-in-kind may damage the international social and physical connectivity at a level that is unacceptable to third parties and the counter-attacker alike. In cyberspace, that collateral damage can be worldwide has been seen repeatedly with the rapid contagion of malware such as computer viruses. In the intermediate case of cyberterrorism, the recent behaviour of the United States with respect to "illegal combatants" in its "war on terrorism" suggests that the model of deterrence at the level of civil and criminal penalties fails here also.

While the difficulties of deterrence may encourage the pursuit of perfect technological defence against cyber attack, the history of every other kind of weaponry cautions that what is at heart a socio-political problem must ultimately be dealt with at a socio-political level. On the political side, the grave potential of international cyber conflict calls for immediate attention. The dual use nature of the technology precludes the kind of international control regime used to regulate nuclear technology. What one can hope for (and work toward) is the creation of a transnational legal framework that

---

100 Hacktivism refers to writing or using computer code (hacking) to attack the target's ICT network with the purpose of promoting a political ideology or social goal. Hacktivists frequently defend their actions as acts of protest and civil disobedience. For an example, *see* http://thehacktivist.com/hacktivism.php.

lays down the rules and penalties for cyber conflict in a set of structured, internationally negotiated binding agreements. Such rules must specify the obligations of the signatory nations with respect to controlling non-governmental organizations or networks that physically operate within their borders.

While the jurisdiction over cyberterrorist or cyberespionage attacks may generally be subsumed under the general criminal civil laws and associated jurisdictional considerations, certain of their characteristics may argue for special laws that *per se* give rise to special jurisdictional considerations. Those characteristics may include: 1) widespread harm with political overtones; 2) increased difficulty in identifying, capturing and prosecuting the perpetrators; and 3) the strong presence of political motivation aimed at societal destabilization in contravention to broadly accepted notions of both criminal law and the laws of armed conflict. There is an additional argument for the special treatment of cyberterrorism. "A special response may typically be justifiable when terrorism is emanating from a group with capacities to organize collectively on a sustained basis, to engage in sophisticated plans and operations and to operate independently from normal life or to have the capacity to intimidate normal society into tolerating its presence."[101] Protracted cyber conflict conducted either for terrorist or military purposes may require or stimulate international coordinated action to limit or control the use of force.

An effective control regime must also codify the actions that may be taken against non-state attackers if, in fact, they can be identified. In the case of terrorist action that originates in the country which has been attacked, action against the attacker can be handled within the context of existing national criminal law, including anti-terrorist statutes. In the case of attacks launched from cooperative or neutral states there are multiple options: 1) extradition to the attacked state; 2) domestic prosecution in a neutral country from which the attack originated; or 3) extradition to a third party that claims universal jurisdiction and generally accepted due process thresholds. Which option to adopt is an issue of balancing considerations of participation of the state of origin, the appearance of justice and the fostering of international intolerance of terrorist methods.

The launching of cyber attacks from rogue or uncooperative countries renders unlikely the availability of normal channels of cooperation in investigation of the attack, the

---

101 Clive Walker, "Cyber-Terrorism: Legal Principle and the Law in the United Kingdom," *Penn State Law Review,* Vol. 110, 2006 at 625-65, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109113#%23.

apprehension and prosecution of the perpetrators, or, where appropriate, extradition. The bottom line issue is whether the attacker(s) will be prosecuted in the state where the attacks were suffered, in a neutral third-party state or in the International Criminal Court. Consequently such cases naturally devolve into issues of intervention by force or by international sanction. These issues parallel those in the case of terrorism by kinetic means. The options open to the country which suffered the attack are

1. retaliatory response against the country;
2. unauthorized entry and apprehension[102] of suspected offenders; and
3. appropriate respect for sovereignty through the engagement of a third-party intermediary state.

Were one to imagine a regime in which certain classes of action in cyberspace were proscribed in analogy with the Geneva conventions regarding kinetic warfare, one might imagine a case of universal jurisdiction in which an international group enters. This possibility raises slippery slope arguments with respect to general lawlessness (and its suppression) on the Internet. Note that the Council of Europe Convention on Cybercrime fails to identify and therefore does not authorize any grounds for cross-border searches of evidence on computer networks, even in hot pursuit.

Concluding Remarks

The accepted facts are: (1) most countries' businesses, governments and utilities are highly dependent on computers and the Internet; (2) although the Internet is intrinsically robust with respect to connectivity, the computers attached to the Internet are far more vulnerable to attack; (3) acquiring fairly powerful attack capabilities currently requires relatively low levels of investment; and (4) definitively identifying the source of an attack is difficult.

With respect to the laws of war, most nations might agree to some general principles as a basis for a harmonized order of cyberspace.

1. Cyber attacks on critical infrastructure are not legitimate weapons of attack even during kinetic war. (Analogies are biological and chemical weapons.)
2. Pervasive, government-funded Internet espionage makes identifying intrusions and disturbances by organized crime, sub-national organizations

---

102 Under U.S. law the means of bringing a suspect into territorial jurisdiction is a not a jurisdictional defense against prosecution.

and hackers more difficult, and it interferes with criminal prosecution of these groups under computer crime laws.

3. Low-level computer espionage by governments may be tolerable, but no sabotage is permitted. Low-level state "competition" spurs technological progress. Moreover, every country has an interest in knowing that the security of foreign military systems is kept safe from potential miscreants.
4. Government spying on foreign private companies has unclear but probably small real world impact. However, it arouses unhealthy nationalistic fervor in citizens, sends bad messages to industry and if done on the behalf of a nation's own private industry tends to create economic power without competition.
5. Since determining the source of an attack and whether it was government-funded is very difficult, disruptive non-governmental entities may be able to instigate national conflict.

Since formal agreements may not be verifiable, an initial goal of international dialogue may be to establish rules of evidence needed to enforce rules of fair play. In this light, assertions about economic advantage or fundamental political dynamics seem to imply a Cold War-type dynamic that would undercut the very goals an international agreement[103] would seek to achieve. More importantly, if they are true, no UN agreement is going to stop this process.

In advancing the goal of mitigating cyber conflict, further intellectual inquiry into the following areas would inform policy discussions conducted in international venues:

1. the theoretical offensive/defensive dynamics of computer security,
2. the offensive/defensive dynamics of computer security development as matter of return on investment,
3. the drag that robust security systems have on operations (computer processing, data storage, system management, human interface time),
4. criminal incentives and deterrence in cross-border crime,
5. the impact of computer espionage on the public and private sectors.

---

103 See the article "A Concept of Cyber peace" by Henning Wegener in this book.

5.2 A Call for Geo-Cyber Stability

By Jody R. Westby

The pace at which cybercrime is increasing cannot be sustained. Rogue actors using botnets routinely exfiltrate confidential and proprietary information and conduct distributed denial of service attacks against government and business systems. McAfee's *2009 Unsecured Economies: Protecting Vital Information* report estimated that respondents lost a combined USD 4.6 billion worth of intellectual property in 2008 and spent approximately USD 600 million repairing damage from data breaches. Based on these numbers, McAfee projected that companies worldwide lost more than USD 1 trillion in 2008. Individuals are burdened with constantly updating operating software and virus protection programs, even though many of their systems are infected and used in attacks.

Nations recognize that their government and business systems are valuable and that their national and economic security is at risk. Thus, they have begun to develop cyberwarfare strategies and establish cyber commands with offensive and defensive capabilities. While such actions are appropriate and to be expected, there is a noticeable vacuum with respect to dialogue concerning cyber peace, much less about maintaining an acceptable level of geo-cyber stability. As noted in the Introduction, the author defines "geo-cyber" as the relationship between the Internet and the geography, demography, economy, and politics of a nation and its foreign policy. "Geo-cyber stability" is defined as the ability of all countries to utilize the Internet for economic, political, and demographic benefit while refraining from activities that could cause unnecessary suffering and destruction.[104]

In part, the reluctance of countries to engage in discussions regarding what "minimum essential communications" are necessary to preserve vital societal functions and prevent unnecessary suffering and destruction from cyber attacks, may flow from a general uncertainty about how such a topic might be approached within the current international legal framework.

---

104 First presented at the ANSER Institute of Homeland Security Conference, "Homeland Security 2005: Charting the Path Ahead", University of Maryland, Presentation by Jody Westby, "A Shift in Geo-Cyber Stability and Security", 6–7 May 2002.

The Laws of Armed Conflict

Throughout modern history, the international laws of armed conflict (LOAC) have been updated in response to the atrocities of war and new methods of war fighting. There is an urgent need to do so again to bring them in line with cyber capabilities because cyberwarfare actions are likely to either violate numerous provisions in existing laws of armed conflict or be outside the scope of the laws all together.

The basic legal frameworks governing armed conflict are extensive and largely were developed over the course of the last century. Key documents relevant to cyber conflict include:

- Charter of the United Nations[105]
- NATO Treaty[106]
- The Geneva Conventions of 1949[107]
- Geneva Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)[108]
- Hague Conventions (1899 and 1907)[109]
- Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects.[110]

---

105 Charter of the United Nations, www.un.org/en/documents/charter/index.shtml.

106 The North Atlantic Treaty, www.nato.int/cps/en/natolive/official_texts_17120.htm.

107 The Geneva Conventions of 1949, www.icrc.org/web/eng/siteeng0.nsf/html/genevaconventions.

108 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 ("hereinafter Protocol I").

109 Convention With Respect to the Laws and Customs of War on Land (Hague II), 29 July 1899, http://avalon.law.yale.edu/19th_century/hague02.asp; Laws and Customs of War on Land (Hague IV), Oct. 18, 1907, http://avalon.law.yale.edu/20th_century/hague04.asp.

110 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, 28 Nov. 2003, www.icrc.org/web/eng/siteeng0.nsf/html/p0811 (hereinafter "Convention on Weapons Excessively Injurious").

The basic premises of these documents can be simplified. The laws of armed conflict regulate the conduct of armed hostilities, and militaries must plan and execute their operations within these laws. They apply to military operations and related activities and are intended to prevent unnecessary suffering and destruction in war. Special provisions protect civilians, prisoners, the wounded and sick, and the shipwrecked.

How Military Actions Can be Conducted

There are three basic principles governing *how* military actions can be conducted: necessity, distinction, and proportionality.

Necessity: The principle of necessity limits combat forces to engaging in only those acts necessary to accomplish legitimate military objectives. Military facilities, equipment, and forces may be targeted if it would lead to the enemy's partial or complete submission.

Distinction: The principle of distinction requires militaries to distinguish between lawful and unlawful targets, such as civilian, civilian property and the wounded. Civilian targets must be separated from military targets to the maximum extent possible. Indiscriminate attacks are considered to be those that strike both military and civilian targets/civilians.

Proportionality: The principle of proportionality prohibits force in excess of that needed to accomplish military objectives. The principle compares the military advantage achieved from the attack to the harm inflicted and requires balancing between the direct military advantage anticipated and the expected civilian injury or damage.

Who Can Conduct Armed Conflict

Only *lawful combatants* can engage in armed conflict. Lawful combatants are persons authorized by a governmental authority to engage in the hostilities. They may be an irregular force but must be commanded by a person responsible for subordinates, have distinctive emblems so they are recognizable at a distance (such as a uniform or color), carry their arms openly, and conduct operations according to the LOAC.

Unlawful combatants are those who directly participate in the hostilities without authorization by a governmental authority or within international law. Civilians who attack forces, pirates, and terrorists are examples of unlawful combatants.

Noncombatants are persons not authorized by a government authority to engage in hostilities, but are involved in them. This group includes persons such as chaplains, civilian personnel accompanying the military, and medical personnel. Noncombatants

may not be the object of direct attack, but they may be killed as an incident to direct attack.

If the status of a combatant is unknown, the Geneva Conventions apply until the person's status is determined.

What Can be Targeted

Military targets are targets that, by their nature, location, purpose, or use make an effective contribution to an enemy's military capability and whose total or partial destruction or neutralization at the time of attack enhance legitimate military objectives.

Protected targets are targets protected by the Geneva Conventions, such as hospitals, transportation of wounded or sick, religious or cultural sites, and safety zones. If any of these targets are used for military purposes, however, they may be attacked. For example, if a military is using a church as their base of operations, it becomes a legitimate military target.[111]

In the cyber context, these principles raise some unresolved questions:

- What constitutes an act of armed cyber conflict?
- Can critical infrastructure be targeted?
- If critical infrastructure supports targets that are protected by the Geneva Conventions, can these networks be targeted?
- Are critical infrastructure attacks necessary to achieve military objectives?
- How can participants in hostilities make such distinctions between military and protected targets?
- Is the damage to the critical infrastructure proportional to the military objectives?
- What is excessive force in cyberspace?
- How are cyber soldiers distinguished?
- How is it determined if third parties are acting for a nation state?

---

111 *See* Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace,* Aegis Research Corp., Falls Church, VA, 2000; *The Law of Armed Conflict: Basic Knowledge,* International Committee of the Red Cross, June 2002, www.icrc.org.

None of the answers to these questions is clear under existing law. For example, are US private sector communication networks a legitimate military target and within military necessity because 90 per cent of US Government communications utilize commercial networks, including the Internet, telephony, cellular, and satellite?[112] The corporations and shareholders owning those networks would surely argue against such reasoning. So would hospitals whose operations are fully dependent upon those networks; they would likely consider such an attack as one against a protected target.

If the LOAC allow the use of irregular forces, can governments hire botmasters and use their botnets as lawful combatants in cyber conflicts? Irregular forces may be authorized to participate in hostilities, but botnets are not recognizable and their arms are not visible.

Certainly, bots in a botnet bear no emblem or mark of distinction. They may not even be traceable to the individual bots because they spread their malware via webpages, peer-to-peer networks, malicious links, social networking sites, and spam. A personal computer functioning as a bot in an attack launched at the behest of a nation state may belong to an innocent civilian who is unaware that their computer has been compromised. If caught, can such botmasters be tried as war criminals? What about the owners of the computers?

The Hague Conventions V and XIII set forth the rights and duties of neutral countries with respect to war on land and at sea, but they are silent with respect to cyberspace. A country may not move troops or convoys across the territory of a neutral nation or commit any act of hostility in the territorial waters of a neutral country, but what about traversing the networks of neutral countries? Are countries required to get permission from neutral countries to send a cyber attack over their networks? With packet switching, how does a country even know what networks will be used? Can a country use a botnet as an irregular force if it involves computers in a neutral country?

The UN Charter, Geneva and Hague Conventions, and NATO Treaty do not accommodate cyber conflict. The UN Charter and NATO Treaty both use terms such as “territorial integrity”, “the use of armed force”, “action by air, land or sea forces” and “armed attack” that do not fit cyber scenarios and seemingly put them outside the reach of international law. The Estonia and Georgian conflicts dramatically illustrate

---

112 *The Insider Threat to U.S. Government Information Systems*, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99, www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf.

the consequences of cyber conflict and the confusion around response efforts caused by uncertainty about the rule of law.[113]

Making the Case for Geo-Cyber Stability

The foregoing discusses only a few legal uncertainties with respect to cyber conflict. A review of the LOAC reveals a historical willingness to update these documents to accommodate new technologies, such as naval weapons and aircraft.[114] Thus, these same instruments could be amended to accommodate cyber conflict.

The first critical question, however, is what degree of activity should be allowed? The author argues that four principles should be applied in circumstances of cyber conflict:

1. *A certain amount of critical infrastructure should be protected to prevent unnecessary destruction, harm, and suffering and ensure minimum essential communications.*

   The critical infrastructures protected would include those that support, for example, hospitals and medical facilities, assisted living centers, financial systems, life support systems and critical medical devices, supply chains, transportation, news reporting, educational facilities, religious churches and centres, first responders and law enforcement. The foregoing list is not meant to be exhaustive, but rather to offer examples of the types of systems that support innocent civilians, including the very young, the infirm and wounded, and the elderly. Stakeholder input should help diplomats define the sacred boundaries of critical infrastructure.

---

113 For a fuller discussion of the Estonian and Georgian conflicts and response and legal issues, *see* Jody R. Westby, "The Path to Cyber Stability," *Rights and Responsibiliites in Cyberspace: Balancing the Need for Security and Liberty",* EastWest Institute and World Federation of Scientists, 2010 at 1, www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

114 See, e.g. "Protection of civilian persons and populations in time of war," extract from "Basic rules of the Geneva Convention and their Additional Protocols", International Committee of the Red Cross, 31 Dec. 1988, www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV (hereinafter "Protection of civilian persons") ("extraordinary developments in aerial warfare has made it necessary to develop and make more specific the existing law of armed conflicts. This is the subject of Part IV or the First Protocol additional to the Conventions."); Geneva Convention II was added to accommodate the use of navies in war and address the treatment of the wounded, sick, and shipwrecked member of the armed forces at sea.

Rationale: The existing LOAC supports this concept. As noted by the *Basic rules of the Geneva Conventions and their Additional Protocols*:

> In any conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited. Two basic rules follow from this principle. The first prohibits the use of weapons, projectiles and material and methods of warfare of a nature to cause unnecessary injury. The second, in order to ensure respect and protection for the civilian population and civilian property, obliges Parties to the conflict to distinguish at all times between the civilian population and combatants, as well as between civilian property and military objectives and to direct their operations against only military objectives.[115]

The harm and damage that would flow from the destruction or incapacitation of critical infrastructure systems is unnecessary and would cause extreme suffering and hardship of the nature that the laws of armed conflict were intended to prevent. Moreover, because these networks service large populations, the harm and damage from such an attack would be widespread and not proportional to the military advantage.

Numerous provisions in Geneva Convention IV support this proposed principle. The Convention specifically addresses the protection of civilian persons and particularly protects the wounded, sick, infirm, and expectant mothers (Art. 16). During hostilities, any party may propose neutralized zones in conflict areas to protect wounded and sick combatants and non-combatants, and civilians who reside in the zones but are neither involved in the hostilities nor performing work of a military nature (Art. 15). Civilian hospitals that provide care to the wounded, sick, infirm, and maternity cases may in no circumstances be the object of attack (Art. 18). Children under 15 years of age who are orphaned or separated from their parents should have their maintenance, religion, and education facilitated (Art. 24). Any destruction of real or personal property belonging individually or collectively to private persons, the country or public authorities, or to social or cooperative organizations is prohibited (Art. 53).

---

115 "Protection of civilian persons and populations in time of war", extract from "Basic rules of the Geneva Convention and their Additional Protocol", International Committee of the Red Cross, 31 Dec. 1988, www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV.

Protocol I of the Geneva Convention supplements Convention IV and extends the protection of civilian persons in time of war. Articles 48-59 of Protocol I are particularly relevant. A civilian is anyone who is not a member of the armed forces. (Art. 50). Civilians shall enjoy general protection against the dangers arising from military operations, they shall not be the objects of attack or subjected to acts designed to spread terror or to indiscriminate attacks that are not directed at a specific military object (attacks expected to cause incidental loss of civilian life, injury, or damage to civilian objects which would be excessive in relation to the military objective are indiscriminate) (Art. 51). Civilian objects shall not be the object of attack or reprisals; in case of doubt, the object shall be assumed to be civilian (Art. 52). Acts of hostility shall not be committed against historic monuments, works of art, or places of worship (Art. 53). Attacks against objects indispensible to the survival of the civilian population (such as food, agricultural areas, crops, livestock, drinking water installations and supplies, and irrigation works) are prohibited (Art.54). Works or installations containing dangerous elements shall not be attacked, such as dams, dykes, and nuclear facilities, even if they are legitimate military objectives if it would cause the release of "dangerous forces and consequent severe losses among the civilian population" (Art. 56). Constant care shall be taken to spare the civilian population (Art. 57). Planners of an attack should take all precaution to verify that the objects of the attack are not civilian or civilian objects or subject to special protections and shall take all feasible precautions to avoid and minimize incidental loss of civilian life (Art. 57). It is prohibited to attack non-defended localities (no military operations or personnel in the area) (Art. 59).

Additionally, the LOAC contain numerous provisions that have been added over the years to ban the use of technologies that are excessively injurious or would have indiscriminate effects. As far back as 1899, declarations to the Hague Convention were adopted banning the launching of projectiles and explosives from balloons "or by other new methods of similar nature",[116] the use of projectiles involving the diffusion of asphyxiating or deleterious gases,[117] and the use of expanding or flattening bullets.[118] In 2001, the

---

116 Declaration, Prohibiting Launching of Projectiles and Explosives from Balloons (Hague, IV); 29 July 1899, http://avalon.law.yale.edu/19th_century/hague994.asp.

117 Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases, The Hague Conference of 1899, 29 July 1899, http://avalon.law.yale.edu/19th_century/dec99-02.asp.

Convention on Prohibitions or Restrictions on the Use of Conventional Weapons Which May be Deemed to be Excessively Injurious or to have Indiscriminate Effects was adopted, which banned a broad range of particularly dangerous and harmful weapons, including those noted above reaching back to 1899, as well as landmines, booby-traps, incendiary weapons, blinding laser weapons, and explosive remnants of war.[119] This convention could be amended to include cyber attacks against defined critical infrastructures.

2. *The use of botnets and other irregular cyberforces should be outlawed.*

Rationale: To the victim, at the beginning of an attack, these combatants are indistinguishable from any other attacker; the victim does not know whether the person attacking their system is an insider, a lone hacker or rogue actor, a sophisticated organized criminal, a terrorist, or a nation state. Tracking and tracing cybercriminal activities is difficult and attribution sometimes cannot be determined, even with skilled investigators and researchers working on the case. Additionally, it is impossible to distinguish a third-party cyber soldier because they cannot wear a distinctive emblem, and they certainly are not distinguishable from a distance. Thus, irregular cyberforces violate one of the basic rules of armed conflict.

3. *Countries must respect the neutrality of other countries and shall not transmit any kind of attack through their critical infrastructures.* (Hague Conventions V and XIII).

This is consistent with the Hague Conventions that restrict the transport of troops or convoys of supplies or munitions across neutral territories or waters. Many critical infrastructures, such as electrical grids, can be destroyed through overloads to the system. Thus, allowing countries to conduct cyber attacks that could transit over many other nations' networks without their knowledge is simply inconsistent with the history and intent of the LOAC. This proposed principle would require countries to obtain the permission of other countries before launching a cyber attack, thereby also working as a deterrent against waging cyber conflict.

---

118 Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body, The Hague Conference, 29 July 1899, http://avalon.law.yale.edu/19th_century/dec99-03.asp.

119 Convention on Weapons Excessively Injurious.

4. *Countries must assist one another in their investigation of cybercriminal activities.*

The cooperation of Internet Service Providers (ISPs) and other governments in the investigation of cybercriminal activities is critical to ensuring some measure of geo-cyber stability. While it may seem counter to require a neutral country to assist in an investigation, even in times of war, all cyber attacks look the same at their onset. It is only through investigation that the victim can gain insights into who the attacker might be. As a basic principle, countries that want to be connected to the Internet should have an obligation to ensure that they, and the providers within their borders, assist in cybercrime investigations. If countries were allowed to refuse such assistance under the cloak of neutrality, all cybercriminals would have a grand time looting the countries involved in hostilities. In a reverse sense, the neutral countries could actually be aiding and abetting either the criminals or the attacking country by refusing to assist. In cyber attack scenarios, it is only through assistance, that a country can remain truly neutral.

Realizing Geo-Cyber Stability

The Internet has created a cyber planet that does not recognize traditional borders and operates largely outside the control of governments. It constitutes a new form of weaponry that presents unprecedented risk to civilians, especially those who are very young, old, sick, fragile or disabled. It also stands the laws of armed conflict on their head because, in cyber conflict, the targets are more likely to be civilian rather than military and impact civilian populations rather than military troops. In most countries, the critical infrastructures are owned and operated by the private sector. Therefore, attacks on critical infrastructure will equate to attacks on civilian populations and the very networks that sustain their lives and livelihoods. The urgency of the need to update the laws of armed conflict to accommodate this new threat cannot be ignored because the *lack of* a legal framework is too easily interpreted as legal approval to attack.

Some legal and security experts call for a grand law or treaty on cyberspace. This is nonsense. Throughout the development of navies, air fleets and other technologies, the LOAC have adapted and remained a consistent, but evolving, body of law. In addition, there are pragmatic considerations. Treaties are problematic; they require long, multilateral discussions in the drafting phase, followed by an opening for signature. Signatories then have to ratify the treaty and implement it into national law. Usually a certain number of signatories must ratify the treaty before it goes into force, and even then, it is only effective for those countries that have ratified and

implemented it. All of this takes time that rogue actors and cybercriminals will find advantageous.

Existing instruments, however, such as the UN Charter, NATO Treaty, Geneva Convention, and Hague Convention all have the ability to be amended *and* they have the advantage of already having been ratified and implemented into national law.

In cyberspace, where minutes matter, the obvious solution is the one that is most expedient. Nation states must come together, with the input of stakeholders, to make the following amendments to existing international laws of armed conflict:

1. The UN Charter should be amended to accommodate cyber conflict and clarify that "territorial integrity" includes critical infrastructures and cyber availability, integrity, and confidentiality. Specifically, Article 42 should be amended to allow Security Council action by cyber means.
2. The NATO Charter should be amended to allow collective defence under Article 5. The term "armed attack" in Article 6(1) should be expanded beyond "territories," and "forces, vessels and aircraft" to encompass cyber attacks.
3. The Hague Conventions should be amended to outlaw the use of irregular forces in cyber combat and prohibit the transmission of cyber attacks through the networks of neutral countries.
4. The Geneva Conventions should be amended to outlaw attacks on critical infrastructure that would impair minimum essential communications and imperil civilian populations.

In one area, a new agreement is needed. Separately, nations must agree to cooperate and assist in the investigation of cybercriminal activities that are believed to have passed through their networks. Countries that are not signatories to this agreement should have no recourse under international law if communications from their country are blocked by other nations.

The foregoing will enable nation states and people to trust ICTs and continue to integrate them into their lives and societies without fear that they will become targets of a cyber conflict. It will also begin a constructive dialogue between nations in which, for the first time, they all come to the table with a common position.

6 Cyber Peace

A Concept of Cyber Peace

By Henning Wegener

This book has been placed under the auspices of cyber peace, in deliberate contrast to the negative phenomena of cyberwar, cyberterrorism and cybercrime. To opt for the positive side in the war–peace antinomy implies an important change in perspective and scale of priorities, as it orients the mind towards the benefits and positive potential of the Information Society and provides a goal post to that effect, reinforcing the negative connotation of cyberwar and related terms and calamities, and instigating dynamic movement towards a global culture of cybersecurity.

This attempt to delegitimize cyberwar through reversing the perspective is fully aware that digital infrastructures are now all-pervasive, and will unavoidably also be used for hostile, non-peaceful purposes. The overriding objective, then, is to harness such uses and to provide the strictest possible limits for any belligerent application of ICTs. As the very term "cyberwar" is conducive to stimulating military thinking patterns, and to conceiving cyber defence predominantly in terms of military action and techniques ("retaliation"), this chapter will attempt to combat this mental automatism and to substantiate a plea for peaceful behaviour in cyberspace. Yet, it cannot be more than the outline of a conceptual underpinning of cyber peace, in need of being fleshed out over time. Many other sections of this book contribute already to this definitional task.

For a number of years, including in public meetings and publications, the World Federation of Scientists has already placed the concept of cyber peace at the centre of its work,[120] and ITU, specifically through its Secretary-General, has recently contributed to making the concept more concrete,[121] but the term has obviously been used before, although not in the same comprehensive way. The most notable, if specific and limited, and in this case child-specific, use of the term has been made in 2007 by Egypt in promoting a Cyber Peace Initiative program in the framework of the

---

120 See the various references under "publications" and "activities" in www.unibw.de/infosecur, under the latter specifically the transcript of a conference in December 2008, entitled "The Global Internet Crisis: The Quest for Cyber Peace".

121 "UN Chief proposes int'l accord to prevent cyber war," 31 Jan. 2010, www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a.

Suzanne Mubarak Women's International Peace Movement (SMWIPM),[122] with direct reference to the UN Declaration and Programme of Action on a Culture of Peace. The mission of the initiative is to empower youth of any nation, through ICT capacity building, towards internet safety and encouragement of innovation. The term cyber peace also appears occasionally, if unsystematically and undefined, in the activities of the peace research community.

In the present context, cyber peace, understood much broader than by the SMWIPM, is meant to be an overriding principle in establishing a "universal order of cyberspace". If the use of the term has more to do with politics and with political emphasis, with orienting the mind towards the right choices, then it also follows that it must remain somewhat open-ended. The definition cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.

Yet, a basic definition is necessary. The starting point for any such attempted definition must be the general concept of peace as a wholesome state of tranquillity, the absence of disorder or disturbance and violence, – the absence not only of "direct" violence or use of force, but also of indirect constraints. Peace implies the prevalence of legal and general moral principles, possibilities and procedures for settlement of conflicts, durability and stability.

We owe a comprehensive attempt to fill the concept of peace – and of a culture of peace – with meaningful content to the UN General Assembly. Its "Declaration and Programme of Action on a Culture of Peace" of October 1999[123] provides a catalogue of the ingredients and prerequisites of peace and charts the way to achieve and maintain it through a culture of peace. Recalling the Constitution of the United Nations Educational, Scientific and Cultural Organization, which states that "since wars begin in the minds of men, it is in the minds of men that the defences of peace must be constructed", the Resolution describes the elements in an extensive manner, and then sets out action points for the decade until 2010.

Important planks for peace and a culture of peace are not only the non-use of force, and the promotion and practice of non-violence, but a shared set of values and modes of behaviour, international order and lawfulness, positive, dynamic participatory processes and human rights (cited are, among others, adherence to the principles of

---

122 The Susan Mbarek Women's International Peace Movement, The Cyber Peace Initiative, http://smwipm.cyber peaceinitiative.org/.

123 "A Declaration on A Culture of Peace," UNESCO, A/Res/53/243, www.unesco.org/cpp/uk/declarations/2000.htm.

freedom, justice, democracy, tolerance, solidarity, cooperation, pluralism, cultural diversity, dialogue and understanding, promotion of conflict resolution). Apart from the much emphasized ethical ingredients of peace, it is particularly important in a cyber context that the catalogue includes among the peace prerequisites the respect for, and promotion of the right of everyone to freedom of expression, opinion and information as well as access to information. These references are, of course, only indicative; the whole resolution bears an attentive perusal. ITU has recently formulated five principles for cyber peace which also establish specific actions and obligations that will ensure peace and stability in cyberspace. The reader is referred to this list as it is of seminal importance.

The World Federation of Scientists for its part has undertaken to translate the general principles contained therein, as well as other general, UN-approved tenets applicable to the cyber environment in some more detail in its "Erice Declaration on Principles for Cyber Stability and Cyber Peace" of August 2009.[124] The Declaration demonstrates that the achievement of cyber stability and cyber peace are closely intertwined. The Declaration is concise, and concentrates on the essential operational elements of cyber peace. These are the following:

1. All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
2. All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cybercriminals.
3. All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenceless, through violence or degradation.
4. Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based

124 "Erice Declaration on Principles for Cyber Stability and Cyber Peace," World Federation of Scientists, Aug. 2009, www.ewi.info/system/files/**Erice**.pdf.

upon internationally accepted best practices and standards and utilizing privacy and security technologies.

5. Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.

6. Governments should actively participate in United Nations' efforts to promote global cybersecurity and cyber peace and to avoid the use of cyberspace for conflict.

Behind these principles, and especially number six, one recognizes the firm intention to harness the conflict potential in cyberspace. And indeed, a special focus of the quest for cyber peace, in the light of the alarming growth of offensive, "cyberwar" capabilities, needs to be placed on the bellicose aspect of activities in cyberspace, by governments and non-government perpetrators alike.

These problems are treated in detail in other parts of this book. Yet, a few statements of principle are in order in the present context of clarifying cyber peace. Cyberspace is as yet, in too large a measure, a law-free space, allowing a free-for-all without guidelines or sanctions, and seemingly giving licence for legally unfettered action. Hence the call for common codes for cyber conduct in all areas of digital endeavour. The World Federation of Scientists has since 2001 called for work on a universal Law of Cyberspace, preferably under the auspices of the United Nations.[125] Nowhere is this more pertinent than in the area of offensive, military uses of cyberspace.

The complexity of this task, and the legal and – perhaps before all – political obstacles on this path are evident. As pointed out elsewhere in this book, the traditional laws of war and armed conflict are ambiguous or even of very limited usefulness, and definitions are lacking. References to traditional limits of action in the principal texts of international law, like those in the UN Charter or the NATO Treaty are largely unavailing. The body of the Geneva Conventions and some UN General Assembly resolutions and conventions, e.g. in the field of transnational organized crime, terrorism or behaviour in outer space, allow for tenuous and incomplete analogies at

---

125 *See Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report and Recommendations, World Federation of Scientists Permanent Monitoring Panel on Information Security, Nov. 19, 2003, Submission to the World Summit on the Information Society, www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf.

best.[126] "Arms control" or the delineation between legitimate and "illegal" use of ICTs, or between offence and defence, are hazy, as the technologies are identical, and the "dual use" problem that besets arms control in so many aspects here becomes endemic. In addition, the tracking-and-tracing dilemma – attribution of authorship, reliably and in suitable timeframes – which already makes the pursuit of "simple" cybercrime problematic, is enhanced in the military domain by the likelihood that a bellicose attacker will maximize sophisticated evasion and dissimulation techniques. Verification, an essential ingredient of arms control, is practically impossible. Deterrence in its traditional sense is not viable when its basic requisites (attribution, location of origin, level of response) are missing. It is thus logical that strong voices in the literature argue that betting on cyber defence (including "extended" cyber defence to allies) rather than on cyber deterrence *per se* is the most appropriate option.[127]

Nevertheless, if one takes the cyber peace concept seriously, a legal framework is essential for defining what constitutes a breach of peace, and States should not be hypnotized by the imperfections inherent in such a framework. In his concept, the Secretary-General of ITU, taking it further from the five ITU Principles, has suggested that nations in such a document should commit themselves not to execute a first cyber strike against another nation ("non-first use"), and should undertake not to harbour cyberterrorists and attackers in their country unpunished.[128] Nations could also be encouraged to conclude, bilaterally or multilaterally, non cyber aggression pacts. There could be mutual commitments not to attack critical national infrastructures (especially those with a humanitarian purpose or serving basic human needs, which would, in part, already be protected by current international law) and could confirm the inviolability of transfrontier data networks. A momentous and courageous step would be, in an international instrument, to delegitimize offensive cyber weapons and offensive strategies for their use.

---

126 Tenuous, but by no means insignificant. *See* Sergei Komov, Sergei Korotkov, Igor Dylewski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law," *ICTs and International Security*, United Nations Institute for Disarmament Research, 2007, www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?fecvnodeid=128420&dom=1&groupot593=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&fecvid=21&ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&v21=128420&lng=en&id=47166.

127 See, for example, Martin C. Libicki "Cyber deterrence and Cyberwar", Santa Monica, 2009, p. 158 et. seq.

128 See Chapter VII.

Realistically, such strategies and principles designed to promote cyber peace will in all likelihood not be able to count on the spontaneous support of the many nations that have already heavily invested, and continue investing, in a cyberwar potential, availing themselves of the current legal vacuum in cyberspace. Indeed, current reports about the systematic "weaponization" of cyberspace, the creation of cyber commands, the development of offensive cyber strategies, etc. are by no means reassuring. Yet, the moral implications of multilateral counter actions should not be underestimated. Legitimacy is an important tool of statecraft, and the mere fact that borderlines for action are drawn, and yardsticks established and agreed, could over time create momentum and motivation. Cyber peace, in order to contribute to cyber stability and fundamental rights, needs determined implementation action.

There is a powerful rationale to invoke for this purpose. The functioning and stability of the interdependent global network structure, and the confidence placed in them is a common public good. Massive cyber attacks even in only a segment of the system are difficult to control, their consequences could be incalculable; there is an built-in tendency for unleashing chain reactions even from modest events.[129] They could decisively alter the power equations, the geo-stability of the entire digital environment on which society depends, much beyond the mere parties to a conflict. The interest in the maintenance of transnational networks and information structures is an interest shared by all international actors.

It needs no argument that unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace.

But the concept stands its decisive test when it comes to defining and evaluating *reaction* to expected or real cyber attacks, in case cyber conflict *does* occur. Whether – or when – a cyber attack is understood to be an armed attack or not: there is general agreement that the overriding international law principle of the right to self-defence *in its generic sense* of the legitimacy of protecting oneself and staving off the onslaught obtains. As has been pointed out repeatedly in this book, defining hostile action as "armed attack" is, in terms of the UN Charter, the NATO Treaty and general international law, the necessary trigger for enabling legitimate individual and collective defence *by military means*. Surely the argument can be made that a cyber

---

129 "The international community needs to be aware that a small cyber-skirmish could be the precursor to a major cyber conflict that potentially will spark a regional kinetic engagement that will have international repercussions." Quote from John Bumgarner, Chief Technology Officer, US Cyber Consequences Unit, *Jane's Defence Weekly*, 29 Sept. 2010, www.jdw.janes.com (hereinafter "Jane's").

attack on another State or with effects in another State, is such an "armed attack" or its equivalent, at least when entailing major destruction or loss of human lives.[130]

This could then provide the legal basis for collective action, including by military means. But the definition and opportunity of military retaliation action in a digital technology context requires careful new thinking and, in the last analysis, a policy of deliberate restraint.

The differences between cyber conflict and traditional – kinetic – "warfare" are striking and go beyond the obvious difference in the "weaponry" used. Summing up arguments proffered in many other sections of this book, including in this very chapter, there is, in the first place, the uncertainty in attribution, and levels of attribution, of cyber attacks, thus making the addressee of any countermeasures or retaliation uncertain – against whom can it be legitimately directed? Then there is, owing to the all-pervasiveness and interconnectedness of digital networks and systems, the unpredictability of the consequences of digital countermeasures and therefore the difficulty of scaling the escalatory effect of any countermeasure. Thirdly, cyber conflict can erupt in a major coordinated and therefore crippling attack, or it can take the form of a pervasive underlying state of perpetual low-level threats (cyber espionage, creation of unrecognized botnets, etc.) with varying degrees of potential to mature into a far-reaching disintegration of infrastructures. In the context of a state-to-state conflict, there is also the novelty of having an infinite number of possible actors; the teachings of the Cold War of the second half of the past century, the functioning of a military-nuclear balance between two powers with its unique blend of deterrence and restraint, cannot simply be transposed to a hostile multi-actor scenario. Finally, as has already been underlined, there is the shared interest of all in the preservation of a functioning world information infrastructure.

These differences, and others that could be cited, must shape our thinking about responses to attack. Under the concept of cyber peace, priority must be given to the maintenance or early restoration of a peaceful and stable environment. That clearly places the emphasis on defence.

---

130 At the time of this writing, NATO nations, in preparation for a summit meeting of the States parties to the Washington Treaty (20 Nov. 2010) are contemplating collective decisions on new threats, including cyber attacks. Should such attacks be subsumed under the trigger actions for collective defence, Art. 4 (mutual consultations), and Art. 5 (mutual assistance by taking such action as "deemed necessary, including the use of armed force") would apply.

Preventive self-defence is the clue to peace-compatible responses. Under this concept, a shared responsibility of all digital stakeholders in equipping themselves with secure networks and systems should be acknowledged, a requirement also stipulated in the Erice Declaration. Company-government collaboration is as important as international cooperation. The key term is resilience: not only the quality of systems, but also their management must contribute to robustness and impermeability to attack. Stakeholders should optimize the situational awareness of their networks, identify high-value assets and address their vulnerabilities (real time monitoring of the entire network, implementation of secure zones, network segmentation, ensuring energy security). Resilient systems and software, rigorously respecting ITU and national security protocols and standards, should, as a consequence, be made widely available. Resilient IT infrastructures discourage attacks, and contribute to a peaceful environment. Superior defence is an essential element of cyber stability; superior defences deter attacks, just as they contribute to trust, and to allowing operators to feel comfortable.

Resilience, as generally defined, includes several elements, among which are the self-healing quality of systems, the availability of warning systems, built-in redundancies, but also trained behavioural modes like the exploration of areas of cooperation within the stakeholder community as part of a peaceful environment, increased information sharing, in short, an emphasis on positive action and inherent encouragements to practice it. Among States considering, and wishing to counter, possible cyber conflict scenarios, high-level regulatory activities might also be considered, like non-cyber aggression understandings, arrangements for transparency to defuse enemy images, malevolence monitoring, and information sharing allowing better attribution to perpetrators in case of conflict. Several of these proposals are also included in the previously cited proposal by the Secretary General of ITU. The nascent global early warning mechanism (the Global Response Center (GRC), the Network Early Warning System (NEWS) or ESCAPE) are of obvious value in allowing for non-violent responses. International cooperation frameworks should use the increasingly extensive CERT networks.

Provision must nevertheless be made for serious cyber conflict scenarios where a mere passive defence posture does not suffice, and the right to self-defence under international law has to be invoked in an active sense. From a cyber peace perspective, here again simple analogies to the traditional law of armed conflicts would be inappropriate. They harbor the risks that the mental framework thus created leads to retaliatory military war scenarios and the military logic of maximizing destruction of enemy assets. The recourse to inherited Rules of Engagement could produce perilous results. Cyber peace does not require renouncing offensive

counteraction and retaliation entirely, but nuances the applicable scenarios in a major way.

Here the key term in devising responses would be *restraint.* Its elements would include a rigorous and continual threat and risk analysis to prevent uncontrollable consequences in terms of disenabling overarching cyber networks; concentration on well-chosen non-escalatory responses; patience and timeliness in responding in order to allow improved attributability of the attack and the activation of redundancies and peer defence alliances; meticulous care in applying the principles of proportionality and necessity inherent in the license to self-defence; and careful protection of critical infrastructures of a humanitarian or socially indispensable character.

While it would probably be exaggerated to argue that in responses to cyber attacks defence is *always* the best offence, cyber peace, in the present analysis, does appear to require, along with stringent limits to retaliation, the principle of prioritizing comprehensive self-defence over offence.[131] This principle would fit in with the call for a systematic delegitimization of cyber "weapons" and offensive cyber strategies on the State level as argued above.

131 "Clausewitz couldn't foresee that the best offence in the 21st Century would be a strong cyber-defence." Jane's.

7 The International Response to Cyberwar

By Hamadoun I. Touré

7.1 National Policies and Approaches

Countries around the world are responding to the new threat of cyberwar in a number of ways. Although some states are just beginning to address the issue of cybersecurity,[132] most governments at the very least recognize the need for reallocation of resources and reform of national security strategies on some level. Many nations are increasing funding, research and tactical and diplomatic resources to improve their cybersecurity.[133] Some countries engage in "air-gapping" – attempting to isolate particular networks by not linking them to other systems – to protect critical information structures and systems from attack.[134] The following section assesses the different approaches adopted by various states.

a) Incorporating cyber capabilities into conventional warfare strategy

Some countries are exploring a conventional warfare approach when it comes to cyber tactics, building up cyber offensive weapons and defensive capabilities as well. They view cyber weapons as "force multipliers," to be used primarily in conjunction with more traditional military actions in order to significantly increase their combat potential.[135] Over recent years, the Internet has become an important medium for information and propaganda exchange during armed conflicts. In this regard, many countries view information sabotage on the Internet as a form of military aggression against public morale and they are thus prepared to meet cyber attacks with military

---

132 For example, South Africa only recently (Feb. 2010) announced its intention to begin to formulate a national, coordinated cybersecurity policy. "Notice of Intention to Make South African Cybersecurity Policy," Republic of South Africa, Government Gazette, No. 32963, 19 Feb. 2010, www.pmg.org.za/files/docs/100219cybersecurity.pdf.

133 "Cyberwar: Sabotaging the System – 60 Minutes – CBS News," 8 Nov. 2009, www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml (reporting that the U.S. Congress has allocated USD 17 billion for cybersecurity offensive and defensive initiatives).

134 David Eshel, "Israel Adds Cyber-Attack to IDF," *Military.com,* 10 Feb. 2010, www.military.com/features/0,15240,210486,00.html (hereinafter "Eshel").

135 Kevin Coleman, "Russia's Cyber Forces," *DefenseTech*, 27 May 2008, http://defensetech.org/2008/05/27/russias-cyber-forces/.

force.[136] Recent incidents involving the leaking of classified military documents illustrate why states worry about the potential consequences of cyber vulnerabilities for morale and public support.[137] Some state officials have indicated in the past that they would consider information warfare tactics to be military actions, whether or not they resulted in casualties, and a military response could therefore be warranted.[138]

b) Cultivating cyber tactics as a national resource

Through their reallocation of resources, funding and strategic planning, many countries are treating their digital infrastructure and ICTs as a national resource or strategic asset. Some countries have even explicitly articulated this as a new national policy.[139] Countries have shifted budgetary resources towards cyberspace initiatives, setting aside considerable sums for research and development of cyberwarfare capabilities.[140] Several governments have articulated and begun pursuing integrated national plans to address the new cyberthreat, mobilizing multiple sectors and completely transforming resources and strategy.[141] This kind of transformation could include training (or re-training) military personnel, revamping intelligence services to

---

136 Gregory Asmolov, "Russia: New Military Doctrine and Information Security," Global Voices, 23 Feb. 2010, http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/ (describing Russia's updated military doctrine, which classifies information warfare as a form of military aggression).

137 *See, e.g.*, Jo Biddle, "AFP: Huge leak of secret files sows new Afghan war doubts," 27 July 2010, www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg.

138 *Cyberwarfare*, Congressional Research Service, RL30735, Updated 19 June 2001, www.fas.org/irp/**crs**/RL30735.pdf (quoting a Russian military official who ruled out the possibility of information warfare being classified as non-military) (hereinafter "CRS Cyberwarfare"). *See also* Peter Beaumont, "US appoints first cyberwarfare general," *Guardian.co.uk*, 23 May 2010, www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/ (reporting that the United States has also indicated it might consider using conventional military tactics to respond to cyber attacks) (hereinafter "Cyber General").

139 President Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House, 29 May 2009, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (stating that that the country's digital infrastructure would now be viewed as a "strategic national asset" and that its protection would be a "national security priority").

140 Iran (estimating Iran's cyberwarfare budget at around USD 76 million).

141 Gurmeet Kanwal, "China's Emerging Cyber War Doctrine," at 20, Journal of Defense Studies, 2009, available at: www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf (discussing China's Information Warfare and Acupuncture policy). [Hereinafter "Kanwal"]

focus on collecting relevant scientific and technological information and conducting cyberwarfare simulations and military exercises, all with specific attention to the applications of information technology.[142] Several countries have initiated national competitions to identify and recruit the strongest cyber minds among their civilian population.[143] Domestic industries are also pushed to develop improved technological capabilities in support of the new military strategy. Some governments are also working to cultivate a pool of private civilian hackers who could be called upon if necessary.[144] These "hactivists" may be tech-savvy individuals or even former illegal hackers recruited and trained to use their skills for national security purposes.[145] Some countries may even use proxies, hired hackers and specialists from other countries who act on their behalf.[146] All of these changes demonstrate a departure from more reactive strategies to cyberthreats and a reorientation around the development of proactive information warfare tactics to effectively act under high-tech conditions.[147]

c) Building cyber military outfits

Several countries have responded to the new threat of cyberwar by allocating large numbers of military personnel to the task of virtual combat.[148] This policy shift could involve the development of Internet warfare teams dedicated to cybersecurity, which could be integrated into other intelligence agencies,[149] or even the creation of entirely

---

142 Cyberwarfare: An Analysis of the Means and Motivations of Selected Nation States, Dartmouth College, Institute for Security, Technology, and Society, Nov. 2004 at 2, www.ists.dartmouth.edu/docs/execsum.pdf (hereinafter "Selected Nations").

143 *See, e.g.,* Richard Westcott, "UK Seeks Next Generation of Cybersecurity Specialists," *BBC News*, 26 July 2010, www.bbc.co.uk/news/technology-10742588.

144 Kanwal at 20.

145 Gordon Corera, "Cyber-security strategy launched," *BBC News,* 25 June 2009, http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm?ad=1 (hereinafter "Corera"); Tom Gjelten, "Cyberwarrior Shortage Threatens U.S. Security," National Public Radio, 19 July 2010, www.npr.org/templates/story/story.php?storyId=128574055.

146 Eshel.

147 Kanwal at 20.

148 Some countries have disclosed their massive personnel shifts. *See* Cyber General (stating that the United States announced reassignment of 30,000 troops to cyber combat). However, information on many countries' strategies is less accessible. See Robert McMillan, "Black Hat Talk on China's 'Cyber Army' Pulled After Pressure", *InfoWorld,* 15 July 2010, www.infoworld.com/print/130362.

149 Eshel.

new sectors within the military structure dedicated to cyber activity.[150] These new military outfits set out to integrate and prepare military resources for full-spectrum cyberspace operations.[151] While their primary focus is often the protection of military networks and conducting military operations in cyberspace, they may also be charged with securing private networks, which power large portions of many military operations, as well.[152]

d) Using cyber tactics to level the playing field

By perfecting information and electronic warfare tactics, some countries hope to level the playing field with nations that rely on software and computer systems to mobilize their conventional armed forces. This transition involves investment in new automated command systems, including hardware such as fibre optic cables, satellites and high-frequency digital radio systems, as well as an increased focus on space, air, naval and ground-based surveillance systems.[153] Some governments already utilize ICTs, in conjunction with tech-savvy military personnel, to monitor national borders.[154] New cyber-oriented strategies might rely even more heavily on these resources, and their attendant automated systems, to secure borders. Other tactics might include command and control operations that focus on disrupting enemy information flow and the targeting of enemy ICT infrastructures to damage and destroy critical machinery, networks and data.[155] These changes focus on attacking potential adversaries' weak points – namely, their reliance on cyberspace and new technologies. Countries that have the strongest traditional and cyberwar capabilities may actually be most vulnerable because of the technology that fortifies them, which is susceptible to

---

150 For example, the United States announced the creation of a new cybermilitary unit in 2009. Cyber General. The United Kingdom also recently announced the creation of a cybersecurity operations center as part of its cybersecurity strategy. Corera.

151 See "U.S. Cyber Command Fact Sheet," U.S. Department of Defense, 25 May 2010, www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

152 Siobhan Gorman, "U.S. Backs Talks on Cyberwarfare," *The Wall Street Journal*, 4 June 2010, http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html (noting that 90 per cent of U.S. military power is provided by the private sector, according to U.S. military officials) (hereinafter "Gorman").

153 Kanwal at 16.

154 Kanwal at 14.

155 Kanwal at 18.

new kinds of attack like logic bombs and hacking.[156] By capitalizing on the potential asymmetry of actions in cyberspace, countries hope to neutralize the military capabilities of their adversaries.[157]

e) Educating citizens and raising awareness of cybersecurity problems

Many governments recognize public education and awareness as powerful methods of cyber defence.[158] Information databases and national awareness months hosted by government or private entities help to boost awareness at the grass roots level.[159] These programs often focus on educating individual users and smaller companies about how to protect their information and systems from cybercrimes such as identity theft and hacking. In most cases, illegal access to the computer system is only a vital first step, and hacking of individual computers or systems can be a precursor to further crimes affecting national security, such as data espionage or denial of service attacks. When carried out against vital national resources or government organs, these "crimes" may be more appropriately characterized as cyber attacks or warfare. Hackers already attempt to infiltrate governments, private businesses and national defence systems on a regular basis, with notable success.[160] Data espionage, or the accessing of sensitive information, can be accomplished through both technical means as well as "social engineering," a tactic which relies on human interaction to trick people into providing access to otherwise secure systems.[161] Therefore, public education about the use of both social engineering and technical methods, such as

---

156 Radical Change ("Because the United States is the most Internet-dependent and automated . . . it's also the most vulnerable to cyberattack.").

157 Kanwal at 18; CRS Cyberwarfare at 11.

158 *See e.g.,* Selected Nations at 5 (recommending systematic and sustained efforts to change the way the U.S. populace views network security in order to improve national cybersecurity).

159 For example, Mauritius' National Computer Board, under the purview of its Ministry of Information and Communication Technology, oversees a Cybersecurity Awareness Portal, available at: www.gov.mu/portal/sites/ncbnew/main.jsp, and the United States observes a National Cybersecurity Awareness Month each October. Public-private partnerships, like the U.S. National Cybersecurity Alliance, also educate users and administrators of digital infrastructure on how to build resilient systems and protective mechanisms. *See* "About Us," The National Cybersecurity Alliance, www.staysafeonline.org/content/about-us.

160 *See, e.g.*, Understanding at 20 (listing famous targets of various hacking attacks, including the Pentagon, the German government, Google, Ebay and NASA). **ITU—this citation has not been listed before. Need full citation**

161 *See id.* at 23–24.

leaving infected thumb-drives in public places, can help to protect national resources.[162]

f) Less connected and developing countries

Although many countries rely heavily on ICTs and the Internet for critical infrastructure and services, other populations are not as dependent or connected, instead using national intranets or resources other than ICTs altogether. However, even these countries appear to be increasing their online capabilities, though such advancements may be limited to military and government uses.[163] Countries that moved online later may face less vulnerability to cyber attacks, as their integral government systems share fewer connections with the rest of cyberspace.[164] But even developing countries that do not yet possess the infrastructure to enjoy the full range of benefits made possible by ICTs still depend on the Internet and other mobile and digital technologies for some of their basic needs.[165] Thus, they too have a stake in the future of cybersecurity.

7.2 Recent International Responses

Today, there exist far fewer international efforts to address the threat of cyberwar than national strategies, although some attempts at multilateral initiatives have been made. Bilateral approaches have also been ventured, but they fall far short of a comprehensive strategy to improve cybersecurity and ensure cyber peace since they only involve a very small fraction of the relevant players in the cyber peace equation. Some countries have called for the creation of a treaty to limit the use of cyber weapons, while others have insisted that such a treaty is either unnecessary or premature.[166] Though these proposals may evidence a step in the direction of

---

162 For example, U.S. Central Command was infiltrated by an infected thumb-drive in 2008. *See* Fifth Domain.

163 Martyn Williams, "North Korea Moves Quietly Onto the Internet," *Computerworld*, 10 June 2010, www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet.

164 Corera.

165 *See e.g.*, "Economic and Social Council Opens General Segment of 2010 Session," at 3, ECOSOC/6444, 16 July 2010, www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm (discussing the "digital cash" or electronic money system used in African countries) (hereinafter "ECOSOC 2010").

166 Gorman.

international collaboration, they too fall short of a truly comprehensive approach and clear strategy for moving forward, one that includes all the relevant stakeholders. The following section introduces some recent international responses, although it is not an exhaustive list.

a) United Nations Office of Drugs and Crime (UNODC) – The United Nations Congress on Crime Prevention and Criminal Justice (UNCPCJ)

In April 2010, the Twelfth United Congress on Crime Prevention and Criminal Justice (UNCPCJ) drafted a set of declarations which included a provision calling for an intergovernmental expert group to study the problem of cybercrime and international responses to it.[167] Accordingly, during the 19th session of the Commission on Crime Prevention and Criminal Justice, the related recommendation was made by its Member States, requesting that the commission establish an open-ended intergovernmental expert group to fulfill UNCPCJ's provision.[168] Although the Congress did not arrive at a consensus on the preparation of a new treaty for cybercrime, it resulted in agreements on technical assistance and capacity building which already form a good basis for discussions on further actions.[169]

b) United Nations Economic and Social Council (ECOSOC)

The UN Economic and Social Council (ECOSOC) opened its 2010 session with a briefing on the challenges of cybersecurity, as well as the threats posed and opportunities provided by ever-expanding use of the Internet. Among other things, the Council emphasized the need for international initiatives which would provide for information exchange, best practices, training and research. In addition, panelists stated that the United Nations must "deliver as one" on the issue, which must increase not only cooperation between countries, but also collaboration between states and the private

---

167 "Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World," Declaration 42, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 18 Apr. 2010, www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529031A_CONF213_L6_REV2_E.pdf.

168 "Report of the Twelfth United Nations Congress on Crime Prevention and Criminal justice", UNODC, Salvador, Brazil, 12–19 Apr. 2010, www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

169 "Summary of outcome regarding cybercrime: 12th UN Congress on Crime Prevention and Criminal Justice," Project on Cybercrime, 26 Apr. 2010,

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/2079_UNCC_cyberoutcome.pdf.

sector to ensure cybersecurity.[170] They cautioned that the international scope and dire consequences of an actual cyberwar require a coordinated response; ad hoc solutions and defence strengthening are now inadequate strategies.[171]

c) North Atlantic Treaty Organization (NATO)

NATO implemented its own policy on cyber defence in 2008 in order to protect its technological resources and those of its member countries.[172] As part of the policy, the alliance created a Cyber Defense Management Authority, a Computer Incidence Response Capability, which provides for the dispatch of Rapid Reinforcement Teams to individual member countries, and a Cooperative Cyber Defense Center for Excellence.[173] Located in Estonia, the Center houses experts who conduct research and training in cybersecurity. Its sponsoring nations include Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic and Spain.[174]

In addition, NATO has also hosted cyber defence exercises, in which teams from member states attempt to defend virtual computer networks from cyber attacks. Such exercises are intended to increase understanding of the international cyber environment and enhance international cooperation for handling technical incidents.[175] NATO has also signed memoranda of understanding related to cybersecurity with Estonia, the United States, the United Kingdom, Turkey and Slovakia.[176]

---

170 ECOSOC 2010.

171 *Id.* (discussing the "digital cash" or electronic money system used in African countries).

172 "Defending Against Cyber Attacks," NATO, www.nato.int/cps/en/natolive/topics_49193.htm.

173 "NATO 2020", www.nato.int/cps/en/natolive/official_texts_63654.htm?selectedLocale=en.

174 Cooperative Cyber Defense Center for Excellence, www.ccdcoe.org/.

175 "Defence exercise to boost skills for countering cyber attacks," NATO-News, 10 May 2010, www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news_63177.htm.

176 "NATO and Estonia conclude agreement on cyber defense," NATO-News, 23 Apr. 2010, www.nato.int/cps/en/natolive/news_62894.htm.

d) Council of Europe – Budapest Convention on Cybercrime

The Council of Europe Convention on Cybercrime[177] addresses certain cybercrimes by providing model legal provisions which countries can adopt and adapt to their specific needs. While the Convention provides some legal solutions to crimes like illegal access (hacking) and interception, it does not address some of the most threatening kinds of cyber incursions, such as data espionage and sabotage. And although the Convention helps to foster international cooperation by criminalizing basic cybercrimes, its prescriptive power is limited by its drafter's attempt not to contravene other potentially conflicting national legislation. Significant cultural and legal differences make the establishment of a unified law slow, if not altogether impossible, under this approach.[178] Only thirty countries have ratified the treaty since its opening for signature in November 2001, with only one of those countries hailing from outside of Europe.[179]

Legal provisions like those set forth in the Convention are one way to address some of the threats to national and international cybersecurity. However, the provisions in the Convention do not directly address the issue of cyberwar between countries. While the threat of sanctions may deter some aspiring cybercriminals, this kind of legislation may not go far enough in deterring attackers who feel confident they can evade detection, identification or prosecution.

e) Bilateral Agreements on Cybersecurity

Individual states are also trying to build relationships with other countries in regard to cybersecurity. For example, the government of India's Ministry of Communications and Information Technology has pursued collaborations in the form of memoranda of understanding or other development and information sharing endeavors with many different countries. For example, India and South Korea signed a joint statement for bilateral cooperation in Information Technology (IT) in 2004 and India's Computer Emergency Response Team also signed a memorandum of understanding with Korea's National Cybersecurity Center to establish formal collaboration in, among other areas,

---

177 Convention on Cybercrime CETS no.: 185, Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last visited on 10 Aug. 2010 (hereinafter "Convention").

178 "National Security Threats in Cyberspace," American Bar Association, Standing Committee on Law and National Security and National Strategy Forum, Sept. 2009 at 13, www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (hereinafter "Workshop").

179 Convention.

cybersecurity.[180] India also has a number of other bilateral understandings related to IT generally and a few focusing specifically on cybersecurity and cybercrime.[181]

Morocco and Malaysia also signed a memorandum of understanding on cybersecurity during the Regional Cybersecurity Conference in Morocco earlier this year.[182] The memorandum created a cooperative relationship between the two countries' cybersecurity ministries, covering areas including critical information infrastructure protection, cybersecurity frameworks development, capacity building, training and awareness. While these kinds of collaborations may improve a country's cybersecurity, they are not enough to protect any one country from a global cyberwar. Therefore, a more comprehensive, global structure related to cybersecurity is needed to ensure peace for all nations.

f) International Telecommunication Union (ITU-T Study Group 17) – Global Standards

To address the growing issue of cybersecurity, in relation to smart grids in particular, ITU has established a Smart Grid focus group that will collect and document information and concepts that would be helpful for developing Recommendations to support Smart Grids from a telecommunication perspective.[183] Focus groups are an ITU instrument that augments the agency's Study Group work programme by providing an alternative working environment for the quick development of specifications in their chosen area.[184] Focus groups are now widely used to address industry needs as they emerge, making them ideal for rapidly changing and developing technologies like Smart Grids. The Smart Grid focus group (FG Smart) consists of representatives from different member states and will collaborate with worldwide smart grid communities (e.g. research institutes, forums, academia). In achieving its objective of providing recommendations for smart grid standards, the focus group will

---

180 "Bilateral Cooperation: Asia," India Department of Information Technology, Government of India Ministry of Communications and IT, www.mit.gov.in/content/bilateral-cooperation (hereinafter "Cooperation").

181 For example, India's collaborations with Brunei, Malaysia, France and Australia specifically focus on information security and/or cybercrime, while other relationships focus on development of resources and facilities. Cooperation.

182 "Malaysia and Morocco Are Now Partners in Cybersecurity," CyberSecurity Malaysia, 24 Jan. 2010, www.cybersecurity.my/data/content_files/44/632.pdf?.diff=1265036362.

183 For more information on the Focus Group, please visit www.itu.int/ITU-T/focusgroups/smart/.

184 ITU-T Focus Groups, available at: www.itu.int/ITU-T/focusgroups/.

maintain a living list of standards bodies dealing with smart grids, collect visions and value propositions for smart grids, provide terminology and taxonomy necessary to support smart grids, gather new ideas relevant to and identify potential study areas to support smart grids, and identify the potential impact of standards development for issue areas such as security, privacy and interoperability.[185] All of these activities will provide a comprehensive and multi-faceted approach to the quickly evolving and increasing cybersecurity challenges related to Smart Grids.

Furthermore, through its connection with the ITU Telecommunication Standardization Sector (ITU-T), one of the most well recognized standards-setting organizations for telecommunications, the focus group will be able to serve as a unifying and reliable source of information and guidance, backed by a reputation for quality, consensus-based standards. The relationship with ITU-T also creates an environment conducive to the progression, if desirable, of the products of the Focus Group, through the Study Group as ITU-T Recommendations, Supplements, Manuals, etc. As part of ITU-T, the Focus Group will be able to achieve greater acceptance of its specifications in many worldwide markets, in particular in developing countries and in regions other than those with more active participation in the particular forum.

7.3 Necessity of an International Framework

a) Non-viability of deterrence

With every new domain come new challenges. Just as the theaters of land, sea, air and space have presented questions of allocation, efficient use and conflict resolution in the past and ongoing today, so too cyberspace creates new obstacles and quandaries. Cybersecurity affects every connected person and, because of the growing reliance on ICTs for basic societal infrastructure, it now affects even those who are not connected. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. Because of the unique characteristics and challenges presented by cyberwarfare, tried and true peace-keeping strategies of the past may no longer prove effective.

Deterrence has long been a favored approach for maintaining peace and security among nations in the face of weapons that could cause massive destruction. But the efficacy of deterrence depends on certain circumstances and assumptions, many of

---

185 Terms of Reference of ITU-T Focus Group on Smart Grid, available at: www.itu.int/ITU-T/focusgroups/smart/tor.html.

which do not apply in cyberspace.[186] Deterrence generally requires four key elements: attribution (knowing who attacked you); location (knowing where a strike originated); response (being able to respond, even if attacked first); and transparency (the enemy's knowledge of your capability and intent to respond with massive force).[187] Cyberspace and cyberwar introduce new problems that undermine the basic assumption that these four elements exist when countries build their military defensive arsenals. ICTs increase the ways in which an attacker can mask his or her identity and location; attackers can use proxies or services like public Internet terminals, wireless networks and prepaid mobile services that do not require authentication. Encryption technology, which is a key technical solution to ensuring confidentiality, integrity and availability, can also be used to mask identities or at least slow the progress of an investigation into the origin of a cyber attack. Technical processes and policies that limit Internet traffic data retention also contribute to this attribution and location problem.

The risk of retaliating against the wrong target, as well as uncertainty surrounding the collateral damage of a cyber counterstrike – which could easily damage an ally or neutral party, further frustrate states' ability to respond to an attack.[188] If attackers believe they can remain undetected or do not believe their victims would respond with military force for fear of straying from international norms, then a retaliatory threat holds very little power. By responding with force to a cyber attack that did not use conventional military force and was intended to exploit more than destroy, a retaliating victim risks the international community interpreting their action as an aggressive and unwarranted act.[189] Relying on a strategy of deterrence also encourages countries to establish threatening postures towards each other and invent new retaliatory threats across different domains to compensate for possible asymmetries, frustrating the benefits of further integration and increasing tensions

---

186 Radical Change (quoting former U.S. security advisor Richard Clarke as stating that, "the force that prevented nuclear war – deterrence – does not work well in cyberwar").

187 Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, The U.S., Russia, India, and Norway,* EastWest Institute, Apr. 2010 at 1, www.ewi.info/system/files/CyberDeterrenceWeb.pdf.

188 James A Lewis, "Cross-Domain Deterrence and Credible Threats," Center for Strategic and International Studies, July 2010, http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf.

189 *Id*.

between nations.[190] In all of these ways, the fundamental characteristics of cyberspace undermine the efficacy of deterrence as an approach to cyber peace.

The very framework of existing legal approaches may no longer be adequate for managing the risks related to cybersecurity. For example, under existing international law as set forth in Article 51 of the UN Charter, a state can legitimately act in its own self-defence when confronted with an armed attack. In the context of cyberwar, this calculus of course begs further questions about when a cyber attack might be viewed as tantamount to an armed attack and, then, whether the attack can be attributed to a nation state.[191] The established doctrine of 'state responsibility' would seem to shed some light on the latter question; it stands for the proposition that every state must act to prevent its territory from being used for attacks on other states and, if it refuses to take preventative action, it can be held responsible for such attacks. However, as we have seen in our preliminary assessments of cyber attacks, this kind of practical question becomes infinitely difficult to answer in cyberspace – some attacks do not have a geographic source (as is the case with "botnets"), they may straddle multiple borders, originate from coalitions located in multiple jurisdictions or be carried out by a proxy who is only acting on behalf of the real perpetrator. Sometimes states themselves may not be able to detect or verify which parties are acting within their own territory. And, even if a state could identify a party acting within its geographic area, the very nature of the cyber domain makes it impossible for any one single entity to exercise complete control.[192] Thus, not only the question of source but also of control becomes unavoidably murky.

b) Necessity of an international framework

Because existing international legal norms and instruments are not fully equipped to deal with the new challenges of cybersecurity, global discussion and collaboration are now necessary. The changing nature of technology itself – with its increasing overlaps between national jurisdictions and their ICTs, online resources and systems – makes the adoption of a new set of strategies, as well as international cooperation, even more critical for ensuring cyber peace.[193]

---

190 *Id.*

191 Workshop at 14.

192 *Id.*

193 *Id.*

Cyber attacks can originate and strike anywhere around the globe, making these threats inherently international in scope and requiring international cooperation, investigative assistance, and common substantive and procedural provisions to adequately address them. Moreover, international cooperation is already widely recognized as one of the key requirements of ensuring global cybersecurity. In 2003 and 2005, nations at the World Summit on the Information Society (WSIS) agreed on the necessity of effective and efficient tools at both the national and international levels to promote international cooperation on cybersecurity.[194] This international collaboration should be motivated not only by a mutual desire for peace, but by each country's enlightened self-interest. Every country is now critically dependent on technology for commerce, finance, healthcare, emergency services, food distribution and more. Loss of vital networks would quickly cripple any nation – and none is immune to cyber attack. The pre-eminence of ICTs and the interconnectedness of developing technologies are thus shaping a new world order, one that calls for collaboration on new issues to ensure stability.

It is critical that countries harmonize their legal frameworks to combat cybercrime and facilitate dynamic, multi-faceted international cooperation. States should work to create a common legal and regulatory framework, and to establish a system for the regular updating of these laws to address the changing nature of security threats. Some groups have already called for the promulgation of international standards and cyber norms as a way of improving international cybersecurity.[195] In any case, an effective strategy for cyber peace must be flexible and adaptable enough to manage and respond to the fast-pace of technological advancement, ICT growth and their attendant security challenges. Countries must also agree on procedures and approaches for tracing points of origin and identities in order to address anonymous cyber attacks and the international entanglements they threaten to create. Proposals for an international agreement requiring every country to police its own cyberspace attempt to address the problem of attribution; tying responsibility to geographic origin might sidestep the messy process of identifying exactly who orchestrated a cyber

---

194 "WSIS: Tunis Agenda for the Information Society," Paragraph 40, World Summit on the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 Nov. 2005, www.itu.int/wsis/docs2/tunis/off/6rev1.html (hereinafter "Tunis Agenda").

195 Participants at a workshop including members of the American Bar Association Standing Committee on Law and National Security, the McCormick Foundation and the National Strategy Forum contemplated the formation of an international Cybersecurity Action Task Force to devise cyber norms and rules to improve cybersecurity. Workshop at 26.

attack.[196] However, these proposals leave unresolved the problems of identifying proxies and of tracing an attack to a geographic location – the correct location. Given the shortcomings of traditional and existing approaches to international security, it is clear that the global community must embrace a new strategy for addressing the challenges of cybersecurity and ensuring a lasting cyber peace.

7.4 Proposals for International Principles in Cyberspace

In promulgating guiding principles for cyber peace, we must consider the distinctive characteristics of cyberspace and the challenges most salient to these features. However, we can still draw from other undertakings aimed at combating similarly transnational threats, such as the Convention Against Transnational Organized Crime, to inform our approach. Like transnational organized crime, cyber attacks span national boundaries and operate through complex networks that parallel or overlay peaceful and productive systems. The Convention illustrates a shared understanding that these pervasive, transnational problems must be addressed by close international cooperation and that they require the adoption of new frameworks, mutual legal and development assistance, information sharing and law enforcement cooperation.[197]

Well-established legal doctrine and internationally endorsed norms support certain necessary elements of a plan for cyber peace. In particular, Article 19 of the Universal Declaration of Human Rights establishes the right to freedom of opinion and expression, which includes the freedom to seek, receive and impart information and ideas through any media and regardless of frontiers.[198] In its 2003 Geneva Declaration of Principles, the World Summit on the Information Society (WSIS) reaffirmed the notion that freedom to communicate is an essential foundation of the Information Society.[199] The Declaration further highlights the role of communication as a fundamental social process and a basic human need that serves as the foundation of

---

196 Robert Mullins, "'Pearl Harbor' post struck a nerve," *NetworkWorld*, 11 Mar. 2010, www.networkworld.com/community/node/58450 (quoting former US presidential security advisor Richard Clarke at a recent cybersecurity panel discussion).

197 Convention Against Transnational Organized Crime, United Nations Office on Drugs and Crime, 2004, www.unodc.org/unodc/en/treaties/CTOC/index.html.

198 Universal Declaration of Human Rights, Article 19, U.N. G.A., Res. 217A (III), U.N. GAOR, U.N. Doc. A/810, 1948, www.un.org/en/documents/udhr/index.shtml#a19.

199 Geneva Declaration of Principles, Para. 4, World Summit on the Information Society, 2003,: www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

all social organization. Accordingly, all people should have equitable access to information and communication technologies. The United Nations has articulated its commitment to ensuring this access to everyone and to fully harnessing the potential of the digital revolution towards this end.[200]

Although the differences between nuclear materials and ICTs are numerous, several key similarities make international collaborations to ensure nuclear peace instructive to a strategy for cyber peace. Like cyberspace and ICTs, nuclear energy and technology have a number of peaceful as well as military uses, they have the ability to create devastating damage if used in an attack and, while they could be used against any country, all countries would feel the effect of such an attack.[201] Recognizing the inherently global nature of the threat of nuclear attacks, the international community has sought a multilateral collaborative strategy that involves the creation of a common approach and a shared commitment to nuclear security.[202] Treaties like the Non-Proliferation of Nuclear Weapons Treaty (NPT) illustrate an effective approach to the challenge of preserving peaceful uses of a potentially devastating material that has the ability to cross national boundaries. The NPT assigns responsibility for materials based on territorial jurisdiction or activities "carried out under [a state's] control anywhere."[203] Echoing this approach, forty-seven nations renewed their commitment to secure nuclear materials under their control, to continue to improve security as conditions change and to exchange best practices and practical solutions for security at the 2010 Nuclear Security Summit.[204]

The NPT also emphasizes the benefits of peaceful applications of nuclear technology and the importance of making these benefits available to all states, including developing countries.[205] The treaty stresses the importance of international cooperation, of all states, including the exchange of information and materials to

---

200 "Ban urges greater use of digital technology to improve living conditions," UN News Centre, 17 May 2010, www.un.org/apps/news/story.asp?NewsID=34716.

201 National Statement of the United States, 2010 Nuclear Security Summit, 13 Apr. 2010, www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states (hereinafter "National Statement of the United States").

202 *Id.*

203 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), Art. 3, 1970, www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglish_Text.pdf (hereinafter "NPT").

204 National Statement of the United States.

205 NPT at Preamble and Art. 5.

contribute to the further development of peaceful applications of atomic energy.[206] Furthermore, Article 3 of the NPT binds signatories to certain safeguards that are intended to prevent the diversion of nuclear energy from peaceful uses to nuclear weapons or other destructive uses.[207] The International Atomic Energy Agency, recognized for its experience, expertise and ability to facilitate discussion in a neutral forum, is charged with overseeing the negotiation and conclusion of an agreement among states which will set forth such a safeguard system.[208]

Other relevant collaborations to ensure nuclear peace include the Global Initiative to Combat Nuclear Terrorism, an international partnership of countries committed to working individually and together to implement a set of shared nuclear security principles.[209] These principles include: developing and improving accounting, control and security measures for nuclear substances and civilian nuclear facilities, improving member state detection and control capabilities, preventing safe havens for terrorists, improving member response, mitigation and investigation capabilities in case of attack and promoting information sharing.[210]

International efforts to ensure peace in other new and seemingly limitless realms also strongly promote broad international cooperation. For example, the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space includes among its guiding principles the proposition that all states should pursue cooperation and mutual assistance in the exploration and use of outer space.[211]

Recognizing the growing risk of a cyber attack that could originate anywhere and affect every nation, the ITU Scretary-General proposes five guiding principles for establishing and protecting peace in the emerging cyber world. These principles embody and advance the values and culture of the International Telecommunication

---

206 *Id.* at Preamble.

207 *Id.* at Art. 3.

208 *Id*.

209 "The Global Initiative to Combat Nuclear Terrorism", U.S. Dept. of State, www.state.gov/t/isn/c18406.htm.

210 "Statement of Principles", The Global Initiative to Combat Nuclear Terrorism, US Dept. of State, www.state.gov/documents/organization/141995.pdf.

211 Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (the "Outer Space Treaty"), Principle 6, 1967, www.oosa.unvienna.org/oosa/SpaceLaw/lpos.html.

Union, illustrated throughout its long history as a leader in international standard-setting and regulation. ITU's authoritative International Telecommunication Regulations (ITRs) provide just one example of this tradition of promoting harmonious development, efficient operation and universal access in international telecommunications and technology. The ITRs were created as a new regulatory framework to address emerging issues and challenges accompanying the new landscape in telecommunications materializing in the late 1980s.[212] They were crafted to promote efficiency and development within the context of collaboration, cooperation and equal access, thus exemplifying the ITU tradition. They also reflect the agency's focus on protecting the right to communicate while also avoiding harm to facilities.

ITU Secretary-General's five principles for cyber peace similarly incorporate these core values while establishing specific actions and obligation that will ensure peace and stability in cyberspace. These principles state that:

1. Every government should commit itself to giving its people access to communications.
2. Every government will commit itself to protecting its people in cyberspace.
3. Every country will commit itself not to harbor terrorists/criminals in its own territories.
4. Every country should commit itself not to be the first to launch a cyber attack on other countries.
5. Every country must commit itself to collaborate with each other within an international framework of co-operation to ensure that there is peace in cyberspace.

212 "International Telecommunication Regulations: Final Acts of the World Administrative Telegraph and Telephone Conference", International Telecommunication Union, 1989, www.itu.int/osg/spu/intset/itu-t/mel88/mel-88-e.pdf.

8 ITU's Global Cybersecurity Agenda

By Hamadoun I. Touré

ITU provides a unique global forum for discussing cybersecurity. The agency has played a major role in telecommunications, information security and standards setting in different capacities since its founding in 1865, nearly 145 years ago. ITU understands that the scale and nature of the cybersecurity challenge require coordinated multi-stakeholder action and it is working towards that goal accordingly. In particular, ITU is currently promoting cybersecurity through a range of activities related to standardization and technical assistance to developing countries tailored to their specific needs. In recognition of its long-standing experience, capacity and expertise, world leaders and governments appointed ITU as the sole facilitator of the WSIS Action Line C5, "Building confidence and security in the use of ICTs."[213] Thus, heads of states and other global leaders participating in WSIS, as well as ITU Member States, entrusted ITU to lead the way by taking concrete steps towards curbing the threats and insecurities related to the Information Society. ITU Plenipotentiary Resolution 140 (Rev. Antalya 2006), addressing ITU's role in implementing the WSIS outcomes, instructed the ITU Secretary-General to take all the necessary measures to fulfill ITU's mandate.

Accordingly, in May 2007, the Secretary-General launched the Global Cybersecurity Agenda (GCA) to provide a framework within which all stakeholders can coordinate an international response to the growing challenges to cybersecurity. The GCA is based on international cooperation and strives to engage all relevant stakeholders in a concerted effort to build confidence and security in the information society. Most recently, Member States confirmed ITU's work in this arena at the 2010 Plenipotentiary Conference, reaffirming GCA as the framework for international cooperation in Resolution 130 (Rev. Guadalajara, 2010). The Resolution instructs the Secretary General to continue to review and improve the progress made under its purview. In particular, Member States noted the strengthening of ITU's role in building confidence and security in the use of ICTs, as well as the Union's global initiative in collaboration with the International Multilateral Partnership Against Cyber-Threats (IMPACT) and the Forum for Incident Response and Security Teams (FIRST). The Resolution also resolved to continue to give high priority within ITU to its work regarding the security of information and communication networks.

---

213 Tunis Agenda.

The GCA works to achieve seven strategic goals, which include:

a) Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;

b) Elaboration of global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime;

c) Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems;

d) Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives;

e) Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structure to ensure the recognition of digital credentials across geographical boundaries;

f) Development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above mentioned areas; and

g) Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above mentioned areas.

In order to achieve these goals, the GCA focuses on five pillars to guide its areas of activity. These pillars are:

1. Legal Measures

Organized cybercrime has been on the rise because the Internet has proved to be a low risk, lucrative business arena. This is due to the fact that loopholes in national and regional legislation still remain, even making it difficult to effectively track down criminals. Within the GCA structure, this pillar seeks to elaborate strategies for the development of model globally applicable and interoperable cybercrime legislation. Particularly with its various cybercrime legislation resources, ITU is assisting Member States in understanding the legal aspects of cybersecurity in order to harmonize their legal frameworks.

2. Technical and Procedural Measures

This pillar focuses on measures for addressing vulnerabilities in software products, aiming to devise globally acceptable accreditation schemes, protocols and standards. ITU, and specifically ITU's Standardization Sector (ITU-T) and Radiocommunication Sector (ITU-R), holds a unique position in the file of ICT standardizations and also plays a vital role in addressing security vulnerabilities in protocols. In order to identify cyberthreats and countermeasures to mitigate risks, ITU is working on secure communication services review enhancements to security specifications for mobile end-to-end data communications and considers security requirements for web services and application protocols. ITU's focus and study groups, such as the recently formed Smart Grid focus group, provide effective mechanisms for accomplishing these goals.

3. Organizational Structures

The world has experienced that watch and warning systems and incident response are essential when it comes to responding to cyber attacks, as is the free flow of information, collaboration and cooperation within and between national organizational structures. This pillar, therefore, aims to create organizational structures and strategies to help prevent, detect and respond to attacks against critical information infrastructures. In this regard, ITU is working with Member States to identify their specific cybersecurity needs and assist them in establishing National Computer Incident Response Teams (CIRTs). Also, as part of ITU's collaboration with the International Multilateral Partnership Against Cyber Threats (IMPACT), the Global Response Centre (GRC) plays a pivotal role in realizing the GCA objectives.

ITU and IMPACT formally entered into a Memorandum of Understanding through which IMPACT's state-of-the-art headquarters in Cyberjaya, Malaysia, has effectively become the physical home of the GCA. This collaboration is providing ITU's 192 Member States with the expertise, facilities and resources to effectively address the world's most serious cyberthreats. The close synergies between the five work areas of the GCA and the services and infrastructure provided by IMPACT made this partnership a logical step in the global fight against cyberthreats. Around sixty countries have already joined the collaboration.[214]

---

214 "International Multilateral Partnership Against Cyber Threats", International Telecommunication Union, www.itu.int/ITU-D/cyb/cybersecurity/impact.html.

IMPACT provides emergency response resources to facilitate identification of cyberthreats and sharing of resources to assist member states.[215] The Global Response Centre (GRC) is equipped with a crisis room, state-of-the-art IT and communications equipment, a fully-functional always-on Security Operations Centre, fully-redundant secure data centre, facilities for shift workers, on-site broadcasting centre and VIP viewing gallery. Thus, the GRC plays a pivotal role in realizing the GCA's objective of putting technical measures in place to combat new and evolving cyberthreats. The two prime highlights of GRC are NEWS (Network Early Warning System) and ESCAPE (Electronically Secure Collaboration Application Platform for Experts). The NEWS program helps member countries identify cyberthreats early on and provides critical guidance on what measures to take to mitigate them. The ESCAPE program is one of the specialized tools and systems to which Members States will have access. ESCAPE is an electronic tool that enables authorized cyber experts across different countries to pool resources and collaborate with each other remotely, yet within a secure and trusted environment. By pooling resources and expertise from many different countries on short notice, ESCAPE will enable individual nations and the global community to respond immediately to cyberthreats, especially during crisis situations.

Not only are the objectives and resources provided by this collaboration in line with the five pillars of the GCA, they are also closely aligned with the proposed principles of cyber peace. The resources made available to member states through IMPACT will assist each government in protecting its own people from cyber attack, thus guaranteeing their continued access to communications via the Internet and other ICTs. By joining IMPACT and participating in resource-sharing and discussions with other member states, each state will also be actively pursuing the fifth principle – the commitment to collaborate within an international framework towards ensuring cyber peace. In addition, IMPACT also offers scholarship grants to eligible developing country member states for training courses that will focus on building a pool of resources and acquired knowledge, which trainees can later share with others to build national capacity and expertise in cybersecurity. These scholarships will improve each country's ability to secure its own ICT resources and also to ensure access to its own people.

---

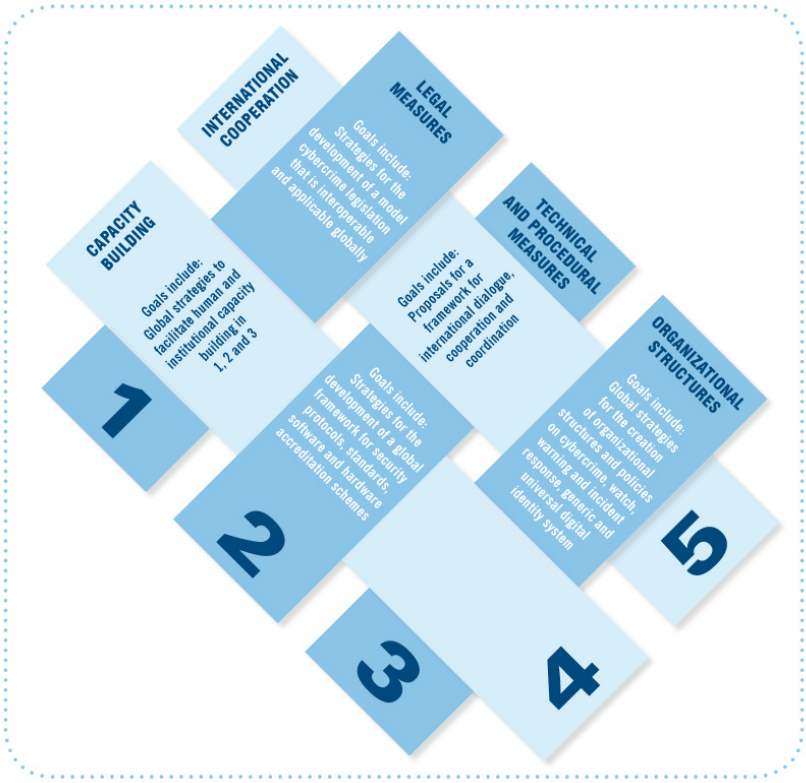
215 ITU Information Letter sent to all ITU Member States on the "Deployment of Cybersecurity Capabilities - IMPACT Global Response Centre", www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf.

4. Capacity Building

Within the GCA framework, this pillar seeks to elaborate strategies for enhancing knowledge and expertise to boost cybersecurity on the national policy agenda. Capacity building needs to be promoted in order to develop a sustainable and proactive culture of cybersecurity. Understanding and awareness of the potential dangers in cyberspace are critical if the end-user is to benefit from ICTs safely. In particular, in line with ITU mandates to assist Member States in developing cybersecurity capacity, ITU works to facilitate the implementation and deployment of cybersecurity capabilities, such as the ITU National Cybersecurity Guide, the ITU Cybercrime Resources and the ITU Botnet Mitigation Toolkit.

5. International Cooperation

Cybersecurity is as global and far-reaching as the Internet. Therefore, the fifth pillar of the GCA focuses on strategies for international cooperation, dialogue and coordination. The IMPACT collaboration represents substantial progress in this direction, providing a platform for member states and third parties to discuss policy and share information. This action directly promotes ITU's mandate from a broad range of member states under the WSIS Action Line C5. The WSIS Declaration of Principles states that strengthening the trust framework, including information and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. In order to achieve this, a global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. The IMPACT collaboration, in addition to ITU's ITRs and focus groups, strengthens this trust framework and works towards these goals by using a comprehensive approach and providing a meeting place for all members of the global community.



Global Cybersecurity Agenda: The five Strategic Pillars

Conclusion

Though the threats accompanying cyber development and the increased dependence on ICTs are grave, the potential benefits are far more compelling. While we have seen some of the risks of cyberwar come to life already, we have also already reaped the benefits of cyberspace – and the possibilities for future benefits are infinite. As we move forward, we must proactively address the question of how we can continue increasing cyber dependence, development and integration, as well as how we can protect resources, create a stable environment for the continued flourishing of infrastructure and new technologies, and ensure lasting peace. Although many existing approaches represent positive steps, they fall short of the mark and may not provide the most effective solution. But there is a strong possibility that if we work together we can accomplish these goals and avoid the dire circumstance of cyber conflict. ITU is already effectively working towards this goal in a number of ways, and it wields the resources and influence required to foster the necessary multilateral support and participation.

9 Erice Declaration on Principles for Cyber Stability and Cyber Peace

By World Federation of Scientists

Erice Declaration on Principles for Cyber Stability and Cyber Peace

It is an unprecedented triumph of science that mankind, through the use of modern information and communication technologies (ICTs), now has the means to expand economic resources for all countries, to enhance the intellectual capabilities of their citizens, and to develop their culture and trust in other societies. The Internet, like science itself, is fundamentally transnational and ubiquitous in character. The Internet, and its attendant information tools, is the indispensable channel of scientific discourse nationally and internationally, offering to all the benefits of open science, without secrecy and without borders.

In the twenty-first century, the Internet and other interconnected networks (cyberspace) have become critical to human well-being and the political independence and territorial integrity of nation states.

The danger is that the world has become so interconnected and the risks and threats so sophisticated and pervasive that they have grown exponentially in comparison to the ability to counter them. There is now the capability for nation states or rogue actors to significantly disrupt life and society in all countries; cybercrime and its offspring, cyber conflict, threatens peaceful existence of mankind and the beneficial use of cyberspace.

Information and communication systems and networks underpin national and economic security for all countries and serve as a central nervous system for response capabilities, business and government operations, human services, public health, and individual enrichment.

Information infrastructures and systems are becoming crucial to human health, safety, and well-being, especially for the elderly, the disabled, the infirm, and the very young. Significant disruptions of cyberspace can cause unnecessary suffering and destruction.

ICTs support tenets of human rights guaranteed under international law, including the *Universal Declaration of Human Rights* (Articles 12, 18 and 19) and the *International Covenant on Civil and Political Rights* (Articles 17, 18, and 19). Disruption of cyberspace (a) impairs the individual's right to privacy, family, home, and correspondence without interference or attacks, (b) interferes with the right to freedom of thought, conscience, and religion, (c) abridges the right to freedom of

opinion and expression, and (d) limits the right to receive and impart information and ideas to any media and regardless of frontiers.

ICTs can be a means for beneficence or harm, hence also as an instrument for peace or for conflict. Reaping the benefits of the information age requires that information networks and systems be stable, reliable, available, and trusted. Assuring the integrity, security, and stability of cyberspace in general requires concerted international action.

THEREFORE, we advocate the following principles for achieving and maintaining cyber stability and peace:

1. All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
2. All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.
3. All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenseless, through violence or degradation.
4. Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and utilizing privacy and security technologies.
5. Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.
6. Governments should actively participate in United Nations' efforts to promote global cyber security and cyber peace and to avoid the use of cyberspace for conflict.

The Erice Declaration on Principles for Cyber Stability and Cyber Peace was drafted by the Permanent Monitoring Panel on Information Security of the World Federation of Scientists (WFS), Geneva, and adopted by the Plenary of the WFS on the occasion of the 42nd Session of the International Seminars on Planetary Emergencies in Erice (Sicily) on August 20, 2009.

10 Conclusion

By Jody R. Westby

To date, the quest for cyber peace has been troublingly quiet. The World Federation of Scientists Permanent Monitoring Panel on Information Security first put forth the concept of cyber peace at a seminal program that it presented at the Vatican's Pontifical Academy of Sciences in December 2008. Subsequently, the PMP drafted the "Erice Declaration on Principles for Cyber Stability and Cyber Peace" in 2009, which was adopted by the WFS and distributed to every member of the United Nations. The concepts and principles put forth in this publication reflect the sobering assessment of the PMP that the world is careening toward cyber chaos, but the path toward cyber peace will result in greater global stability.

The statistics and scenarios presented herein indicate the seriousness of containing cybercrime and cyber conflict. The Internet has created the crime of choice because attribution is difficult and criminals are rarely caught and prosecuted. We fear that the Internet is also becoming the weapon of choice. With easy access to a nation's most sensitive data and critical infrastructure operations, the smallest of countries can take on countries with the largest defence budgets. Developing countries have shown developed nations how to build ICT infrastructure in a non-linear fashion through the use of satellite and wireless technologies. Similarly, countries are learning that cyber exploits present an attractive non-linear option to advancing national and economic security interests.

Why is not cyber containment or cyber peace the mantra of the day? Instead, military leaders around the world are busy announcing their establishment of cyber commands and their plans to develop capabilities to attack, defend, and exploit networks. When countries were faced with nuclear weapons, they began to clamor for containment and non-proliferation. Countries banded together around the globe in the common cause of stopping a global danger that threatened mankind. As the Estonian and Georgian attacks demonstrated, when an attacked country faces a deficient international legal framework, diplomatic uncertainty, technical limitations, and an inability to track and trace communications, the notion of cyber peace becomes rather appealing.

Although numerous multinational organizations are working on various aspects of cybercrime and/or cyber conflict, only ITU has taken a global view and put forth an agenda intended to address major problem areas, while leveraging the efforts of other organizations. The Secretary-General is to be commended for his leadership, vision, and courage to tackle such an enormous problem head-on. We sincerely hope that

other organizations will endorse and emulate this approach and that leaders will step forward to develop a cyber code of conduct and legal framework that supports and advances geo-cyber stability.

We are approaching a dangerous precipice at which time the dark side of the Internet may overshadow the enormous benefits of ICTs and upset world order. The time for cyber peace is now.

Contact Information:
Corporate Strategy Division
International Telecommunication Union
Place des Nations - 1211 Geneva 20
Switzerland
E-mail: strategy@itu.int
Website: www.itu.int/cybersecurity

Printed in Switzerland
Geneva, January 2011