THE QUEST FOR CYBER CONFIDENCE

International Telecommunication Union

THE QUEST FOR CYBER CONFIDENCE

By Dr Hamadoun I. Touré

Secretary-General of the International

Telecommunication Union

and

the Permanent Monitoring Panel on Information Security

World Federation of Scientists

NOVEMBER 2014

Legal notice

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 Henning Wegener, and all the authors who have made it possible to put together their views on this emerging global concern. The Secretary-General expresses gratitude to Prof. Antonino Zichichi, President of WFS. His sincere thanks go to Marco Obiso who led and coordinated this publication and the ITU Cybersecurity team, particularly Alex Gamero Garrido, Aliya Abdul Razack, Despoina Sareidaki, Anthony Drummond, Preetam Maloor and Rosheen Awotar-Mauree as well as many others in ITU and WFS without whose contribution this publication would not have been possible.

If you have any comments, please contact the Cybersecurity team, International Telecommunication Union, at cybersecurity@itu.int.

TABLE OF CONTENTS

Page

About the International Telecommunication Union

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 multi-stakeholder cooperation in cybersecurity aimed at building synergies with current and future initiatives and partners. It focuses on the following five work areas: Legal measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation.

Some key initiatives to assist Members States in building capacity in Cybersecurity under the umbrella of the GCA and with the support of global partners include:

- The National CIRT programme (Computer Incident Response Team) Programme whereby National CIRT Assessments, National CIRT implementations and regional cyber drills are conducted following request from Member States.
- The establishment of Regional Cybersecurity Centres with the aim to serve as catalysts for enhancing regional cooperation, coordination and collaboration to address escalating cyber threats.
- "Enhancing Cybersecurity in Least Developed Countries" project through which ITU assists the LDCs to enhance their capabilities, capacity, readiness, skills and knowledge in the area of cybersecurity.
- The Global Cybersecurity Index (GCI), a measure of each nation state's level of cybersecurity development. The GCI aims at providing the right motivation to countries to intensify their efforts in cybersecurity. The ultimate goal is to help foster a global culture of cybersecurity and its integration at the core of information and communication technologies.

About the World Federation of Scientist

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 cyber warfare 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 Declaration has been distributed to every Member State of the United Nations and is also available, along with all other declarations, publications and internal documents of the Permanent Monitoring Panel on Information Security at its web site: www.unibw.de/infosecur.

The PMP is chaired by Ambassador Henning Wegener. Its members contributing to this publication include:

Contributing Members

Mona Al-Achkar

Dr. Mona Al-Achkar Jabbour has a PHD in private law, and was head of the legal and research departments of the Lebanese University from 1998 until 2009, and consultant and supervisor for implementation of the legal database at the Ministry of Justice in Kuwait.

She is currently professor of law at the Lebanese Faculty of Law, professor- researcher at the Lebanese Legal Informatics Center, founder and president of the Lebanese Information Technologies Association (LITA), founder of Lebanon's Cybercrime Center, member and founder of the Pan-Arab Observatory for Cyber Security, and member of Online Arab writers, the Arab Federation of Online Arbitration, the legal committee for child online protection at the Lebanese Social Affairs Ministry, the "Francophone Team" at ICANN and IGF, the Lebanese Internet Center' (LINC), and the World Federation of Scientists' Permanent Monitoring Panel on Information Security.

Dr. Al-Achkar has published numerous books and articles on various legal issues, some related to legal informatics and cyber law and to money laundering and terrorism.

William Barletta

William Barletta is Adjunct Professor of Physics at MIT and UCLA and Visiting Professor, Faculty of Economics, University of Ljubljana. He is the Director of both the US and the Korean Particle Accelerator Schools and the Coordinating Editor-in-chief of Nuclear Instruments and Methods – A. He also serves as senior advisor to the President of Sincrotrone Trieste, Italy, the co-chair of the Permanent Monitoring Panel (PMP) on Energy of the World Federation of Scientists and as a member of the PMP on Information Security. He is Chair-elect of the Panel on Public Affairs of the American Physical Society (APS). He has been Chair of the APS Forum on International Physics and the Division of Physics of Beams and an active member of the APS Committee on International Scientific Affairs.

He is editor of four books about accelerator science and co-author of four books concerning cybersecurity, privacy and international cyber-law. He holds four patents, and is author of >170 scientific papers. He holds a Ph.D. in Physics from the University of Chicago.

Pavan Duggal

Pavan Duggal is acknowledged as one of the top four cyber lawyers in the world and has made a significant impact internationally as an expert and authority on cyber law and e-commerce law.

A practicing advocate, Supreme Court of India, Pavan has also to his credit pioneering work on convergence law and mobile law. As such, he acts as a consultant to UNCTAD and UNESCAP on cyber law and cybercrime respectively. He is also a member of the AFACT Legal Working Group of the UN/CEFAT, an expert consultant on cybercrime for the Council of Europe, and a member of the board of experts on e-commerce at the European Commission. His work as an expert authority on a cyber law primer for the e-ASEAN Task Force and as a reviewer for the Asian Development Bank is further testimony to his worldwide acceptance as an authority on these issues. In addition, he is the President of Cyberlaw Asia & Cyberlaws.Net.

Pavan has spoken at over 1200 conferences, seminars and workshops, and has written 42 books on various aspects of the aforementioned laws in recent years.

More about Pavan Duggal is available at http://www.linkedin.com/in/pavanduggal.

Solange Ghernaouti

Solange Ghernaouti, Doctor in Computer Sciences (Paris University), is professor of the University of Lausanne and director of the Swiss Cybersecurity Advisory and Research

Group. She is an internationally recognised expert on cybersecurity, cyber defence, cybercrime and ICT risk governance related issues. She has contributed to several initiatives organised by international organisations, public and private institutions, research centres, and law enforcement agencies, among other instances around the world. Her main focus for several years as a pioneer in the field has been on developing an interdisciplinary and integrative cybersecurity approach for citizens, organisations and States.

She is an active independent security advisor and an influential analyst, and a regular media commentator. She has been recognised by the Swiss press as one of the outstanding women in professional and academic circles. Chevalier de la Légion d'Honneur and member of the Swiss Academy of Sciences, she has authored more than 300 publications and twenty eight books including: "Cyberpower: Crime, Conflict and Security in Cyberspace" (EPFL Press 2013); and with Judge Schjølberg "A Global Treaty on Cybersecurity and Cybercrime – A contribution for peace, justice and security in cyberspace" (Cybercrimedata, 2009). She is a member of the World Federation of Scientists' Permanent Monitoring Panel on Information Security.

More information: www.scarg.org

Gabor Iklody

Gabor Iklody is currently working for the European Union's External Action Service (EEAS) in Brussels, as Director for Crisis Management and Planning. Previously, as NATO Assistant Secretary General for Emerging Security Challenges he set up and directed NATO's newest policy Division with responsibility for non-traditional challenges, such as cyber defence, counter-terrorism, WMD non-proliferation and energy security as well as nuclear policy and strategic analysis. He also chaired NATO's Cyber Defence Management Board.

Before his international assignments he worked for almost thirty years in the Hungarian foreign service, most recently as Political Director and Deputy State Secretary in charge of multilateral and security issues. He served two four-year terms in Scandinavia as Ambassador, first in Norway (1999-2003) and later in Sweden (2005-2009). A large part of his career was devoted to Euro-Atlantic integration, multilateral diplomacy and arms control.

Danil Kerimi

Danil Kerimi is responsible for shaping the technology agenda, developing the global public sector outreach strategy and bringing together various ICT-related initiatives under the hyper connectivity platform (cyber security, data, technology for humanity, ICT for competitiveness, internet governance) for the World Economic Forum (WEF).

He manages the involvement of top public sector and industry leaders, knowledge and civil society experts in the ICT projects of the Forum. In addition, Danil is responsible for the Global Agenda Council on Cyber Security and the WEF's Annual Global Information Technology Report. Prior to joining the WEF, Danil had various leadership positions with the United Nations, the Organization for Security and Cooperation in Europe, the International Organization for Migration, and other major international institutions.

Axel Lehmann

Axel Lehmann is a full professor emeritus at the Department for Informatics at the Universität der Bundeswehr München, Germany, where he held a chair for modelling and simulation until 2011. He is now also executive director of the Research Institute for Intelligent Systems (ITIS) at this university. His major areas of research range from computer-based modelling 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 Modelling and Simulation International, , fellow of the German Informatics Society and of the Federation of Asian Simulation Societies, a member of various editorial boards of scientific journals in the fields of modelling and simulation, and a member of international working and standardisation groups as well as of review committees, e.g., for the European Union and for NATO. He is a member of the World Federation of Scientists' Permanent Monitoring Panel on Information Security since its formation in 2001.

Stefan Lüders

Stefan Lüders, PhD, graduated from the Swiss Federal Institute of Technology in Zurich and joined CERN in 2002. As an initial developer of a common safety system used in all four experiments at CERN's Large Hadron Collider, he gathered expertise in cybersecurity issues related to control systems. Subsequently, n 2004, he took over responsibilities in securing CERN's accelerator and infrastructure control systems against cyber threats. He then joined the CERN Computer Security Incident Response Team and is today heading this team as CERN's Computer Security Officer with the mandate to coordinate all aspects of CERN's computer security. This includes office computing security, computer centre security, GRID computing security and control system security, while taking into account CERN's operational needs. Dr. Lüders has frequently given presentations on computer security and control system cybersecurity topics to international bodies, governments, and companies, and published several articles on these issues.

Howard A Schmidt

Howard currently serves as a partner in the strategic advisory firm, Ridge-Schmidt Cyber, an executive services firm that helps leaders in business and government navigate the increasing demands of cybersecurity. He serves in this position with Tom Ridge, the first secretary of the Department of Homeland Security. He also serves as executive director of The Software Assurance Forum for Excellence in Code (SAFECode).

He brings together expertise in business, defence, intelligence, law enforcement, privacy, academia and international relations, gained from a distinguished career spanning over 40 years. He most recently served as Special Assistant to the President and the Cybersecurity Coordinator for the United States. His former White House appointments include Cyber Advisor to Presidents Barack Obama and George W. Bush.

Previously, Mr. Schmidt was the President and CEO of the Information Security Forum (ISF). He previously held positions as Vice President and Chief Information Security Officer and Chief Security Strategist for eBay Inc., and formerly operated as the Chief Security Officer for Microsoft Corp. He also served as Chief Security Strategist for the US-CERT Partners Program for the Department of Homeland Security.

Mr. Schmidt holds a bachelor's degree in business administration (BSBA) and a master's degree in organizational management (MAOM) from the University of Phoenix. He also holds an Honorary Doctorate degree in Humane Letters and is Adjunct Distinguished Fellow with Carnegie Mellon's CyLab and a Distinguished Fellow of the Ponemon Privacy Institute. He previously served as a member of the PSG for ENISA. He currently is a Professor of Research at Idaho State University. He also is a member of the World Federation of Scientist, Permanent Monitoring Panel on Information Security.

Howard is a Ham Radio operator (W7HAS), a private pilot, outdoorsman and an avid Harley-Davidson rider. He is married to Raemarie J. Schmidt, a retired forensic scientist, researcher and instructor in the field of computer forensics. Together, they are proud parents, and happy grandparents.

Hamadoun I. Touré

Dr Hamadoun I. Touré has been Secretary-General of the ITU since January 2007; he was re-elected for a second term in October 2010. He has wide professional experience in both the public and private sectors.

A national of Mali, Dr Touré 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 ITU towards implementing the resolutions of the World Summit on the Information Society (WSIS) and achieving the Millennium Development Goals (MDGs).

Dr Touré is married with four children and two grandchildren.

Henning Wegener

Henning Wegener is a former Ambassador of Germany. He served as Ambassador for Global Disarmament in Geneva (1981-1986), Assistant Secretary-General for Political Affairs at NATO (1986-1991), Director-General at the German Federal Chancery (1991-1994) and thereafter as Ambassador to Spain (1995-1999). Ambassador Wegener has been Chairman of the Permanent Monitoring Panel on Information Security since its inception in 2001, and continues with this assignment, with a short interlude as co-chair from 2009 to 2012. His work has been featured in publications in the field of foreign and security policy, including cybersecurity. Mr. Wegener is a member of the Club of Rome (Spanish Chapter) and serves on the board of several foundations. Among other degrees he holds a Doctor of Juridical Science from Yale Law School. henningwegener@hotmail.com

Preface by ITU Secretary-General Dr Hamadoun I. Touré

This book addresses the increasingly daunting task of building confidence in the use of cyber platforms and technologies against a backdrop of recent high-profile security breach incidents and a plethora of emerging threats that have shaken trust in these essential tools of our time.

It follows publication of *The Quest for Cyber Peace* in 2009, which focuses on the promotion of cyber peace in a sphere which has generated tremendous benefits and progress to mankind, but also spawned widespread criminal activities and created new avenues for intelligence gathering, industrial espionage, and conflict.

Necessarily, this volume returns to these issues revolving around the overriding theme of the use of the cyber domain as a potent force for either good or evil, especially the impact of the 'dark' Internet on trust in the cyber dimension. Here, however, its central theme promotes the concept of cyber confidence. As the introductory chapter points out, it is no longer an exaggeration to speak of a 'crisis of confidence' in the cyber sphere. Indeed, an analysis of recent trends demonstrates that several developments have converged to produce a cumulative negative impact on cyber confidence, among which the growing militarization of cyberspace and the increasing emergence of offensive military capabilities directed not only at military targets, but by cascade effects also at critical civilian infrastructure are particularly preoccupying; the concept of cyber peace was developed to help stem that tide. Of even more topical significance is the unprecedented level of digital espionage and privacy encroachments in cyber space that have recently come to the forefront of public concern.

Throughout the book, the authors, from various angles, evoke these cumulative causes for the erosion of confidence, analyse them, and develop strategies to counter them effectively. In doing so, they focus on three target areas considered crucial to restoring and building this confidence: 1) establishing *normative policy and regulatory frameworks* specifically applicable to the digital age; 2) strengthening *resilience* to withstand the multiple misuses of cyberspace; and 3) ensuring fundamental *freedoms* such as freedom of access and freedom of expression in the cyber realm. In all three areas they also outline and evaluate ongoing initiatives at global, regional and national levels conducive to achieving these goals.

The book is a vibrant call to action to address these issues and presents compelling arguments in this regard. Like its predecessor, *The Quest for Cyber Peace,* it was sponsored and authored by the World Federation of Scientists and the International Telecommunication Union, both organisations at the forefront of this endeavour.

Preface by World Federation of Scientists President Professor Antonino Zichichi

At the outset of the Third Millennium science, more than ever before, is the prime determinant of change and historical evolution. It allows humanity to penetrate ever further into the functioning and secrets of the universe. In the process, complex systems become ever more complex. There are new forms of interaction between human beings and the environment: the relationship of mind and machine undergoes rapid change and needs to be redefined. We enter into a period of unexpected discoveries, but also of unprecedented challenge.

Digital technologies have a role in science and applied science. These technologies and their tools are increasingly all-pervasive, producing an almost unimaginable curve of growth and availability of knowledge, and providing the monitoring devices and control systems for practically all human endeavours. Specialized computer-based applications, distributed computing with grids and clouds, based on highly developed information infrastructures, the evolution of microelectronics and new sensors, the evolving universe of interconnectivity, often automatic, of a myriad of digital devices, and the rapid transformation of manufacturing processes are some of the features of this new era.

Far from enumerating all the countless benefits and opportunities of the digital age, as President of the World Federation of Scientists I would like to underline the importance of science and the evolution of digital technology for the promotion of peace and the mastering of Planetary Emergencies. The effective monitoring of these emergencies depends on real-time collation of information – for prevention, response, recovery and redress. In all of this I am keenly aware of the moral responsibility of the scientist.

Digital space knows no frontiers, its all-pervasiveness has flattened the world and reduced drastically distance and time. The ambiguity inherent in cyber technology as in all modern technologies – that they can serve the good or produce evil – thus has global dimensions. Cyberspace is a domain of immense opportunity, but also of danger, heightened by the absence of adequate, universally valid regulatory frameworks. Hostile uses of digital technologies become increasingly menacing. Cybersecurity and data protection thus become ever more critical core components of digital risk management. They have become a fundamental aspect of the digital revolution, and must become a true growth industry to stem dangerous tides.

The World Federation of Scientists, with its pluridisciplinary group on Information Security, has for more than a decade contributed to this endeavour. A previous joint publication with the ITU Secretary-General placed the emphasis on the secure and peaceful uses of digital technology, – on the Quest for Cyber Peace. This volume deals with another vital aspect of a functioning digital society: trust, confidence. Users, and society at large, must not only be confident that the technology functions unimpaired, but must also be able to rely on the integrity and privacy of digital devices and data, and their underlying network structures. Mutual confidence underpins all meaningful and enduring cooperation. In a global cyber space, in an increasingly interacting global Information Society, this is of crucial significance. Trust makes international interactions more effective and productive by maintaining mutual expectations of good faith and reciprocity. I am grateful to Secretary-General Touré and the co-authors of this volume for having laid out the many dimensions of cyber confidence, and for having formulated the requisite recommendations.

Introduction: The Crisis of Cyber Confidence

By Henning Wegener

Three years ago, the ITU Secretary-General and members of the World Federation of Scientists' Permanent Monitoring Panel on Information Security published *The Quest for Cyber Peace*[1]. That book brought the growing perils in cyberspace into sharp focus, and issued a call to action by all stakeholders in the cyber realm to engage in collective efforts to ensure an adequate level of stability in Internet and digital net structures, and to advance the concept of global cyber peace. Deliberately concise and reflecting a larger state-of the-art public debate, that book has not aged. Its authors, largely identical with those of the current sequel, stand by their analyses and recommendations of the time.

[1] *The Quest for Cyber Peace*, International Telecommunication Union & World Federation of Scientists, Geneva January 2011.

Yet, the situation has become more preoccupying since, and it is no exaggeration to speak of a new dimension of threats in cyberspace that is evolving further before our eyes. The earlier publication centred largely on the preoccupying perspective of cyber conflict, including cyberwar. That perspective has, if anything, become even more worrisome, and has by no means subsided. Necessarily, therefore, cyber conflict figures prominently in this publication; there is thus a clear continuity between the two titles. However, the emphasis of the contributions to this volume has shifted commensurate with the threat development. The central theme of this book is the concept of cyber confidence, with the purpose of analysing the trends that have undermined it to a critical extent, and the strategies and techniques required to restore it[2].

That confidence is an essential prerequisite of a functioning information society based on digital technology is not a new insight. When perusing the documents adopted by the World Summit on the Information Society (WSIS) at its two sessions in 2003 and 2005, one immediately realises that the concepts of trust and confidence permeate the texts and recommendations like a red threat. “Confidence and security are among the main pillars of the Information Society,” we read, and “Building confidence and security” are also the main tasks of WSIS Action Line 5.

In the ongoing post-WSIS discussions, the 2014 Facilitators’ Report for this Action Line states as one of the main areas of concern (the citation is from the Executive Summary): “Strengthening the trust framework: Increasing the level of trust in digital devices, in cybersecurity, and creating a trusted environment between public and private organisations are key challenges. The level of citizen trust in digital services and the Internet must be improved.”[3]

As trust is a central element of the Information Society, its relevance to all segments of the digital world is evident. Thus, although the focus of *The Quest for Cyber Peace* is elsewhere, the book contains an extensive essay on the concept of trust and its all-

[2] In order to demonstrate the continuity between the two publications, the title chosen is *The Quest for Cyber Confidence*. Yet the use of the word Quest is not the same in each of the two cases. In the first book, Quest expresses the longing for a state of peace not yet attained, in the second book, confidence is there, but starkly impaired, and the word Quest aims at its restoration and consolidation.

[3] Doc. WSIS+10/4/2

pervasive role in society[4]. The author stresses: "Trust and trustworthiness are at the basis of human existence," underpinning all social intercourse and enabling people to cope with the high levels of uncertainty and the complexity of contemporary life, thus reducing perceived risk. His analysis provides an overview of current literature on this central concept of societal life. As the book is still publicly available this general reference to his research may suffice[5].

Trust and confidence are largely synonymous, but trust refers more to interpersonal relationships, confidence rather to the relationship of a person with non-human entities or institutions. For our theme, the latter would include digital devices and products in terms of hardware, software, networks, infrastructures, applications, and handling procedures. This publication has therefore chosen confidence as its central term, without being oblivious of the personal expectations and perceptions inherent in the term trust.

As already stated, confidence is a crucial prerequisite of a functioning digital world. But recent events affecting this relentlessly growing digital universe have badly shaken trust and confidence. It is no exaggeration then to speak of a crisis of cyber confidence.

The factors that have combined to produce and foment this crisis are evident, and can easily be enumerated.

- Growing concerns that cyberspace is becoming militarised and that ever more States are developing offensive military capabilities directed not only at military targets, but in effect at an adversary's essential civil infrastructures and civilian modes of life, with uncontrollable overspill effects, and no inhibition to embark on a digital arms race. More than 100 States are presently building up their digital attack capabilities in an unbridled and increasingly dangerous game of strategic reciprocity in which the malicious use of ICT capabilities is clearly announced in relevant doctrines, as a means to achieve military and political goals. These concerns do not preclude the legitimate need for self-defence.
- Despite the primary necessity to adapt International Law to the digital age and to define the limits of hostile use of digital technologies, there is increasing

[4] Jacques Bus, Necessity for Trust: The concept of Trust and its role in society, "*The Quest for Cyber Peace*", p. 17.

[5] The principal authors cited are O'Hara, Luhmann, Hardin, and Fukuyama.

concern that, rather than promoting cyber peace, current efforts to elaborate such normative tools inherently legitimise the large-scale inclusion of cyber weapons in the military arsenals of States, making their operational deployment a normal part of strategic planning;

- Increasing anxieties that civilian infrastructures of vital significance will be attacked by States or non-State actors, be it under the pretext of legitimate military activities or with criminal intent;
- Uncertainty about the rules and behavioural norms that could apply to all these developments, and provide yardsticks and signposts that could help to arrest the loss of and rebuild cyber confidence. This uncertainty is further heightened by the failure of normative efforts over the past decade to produce universal, harmonised codes of sufficiently broad application;
- An ever more complex technical environment with great potential, but also new vulnerabilities and unpredictable consequences for a universe of interconnectivities. Fears are stoked by the exponential growth of digital devices; the additional vulnerabilities caused by the increasing "application" of digital users; the security challenges generated by the migration to mobile and cloud applications; the alarming growth of new malware components[6]; the rising curve of cybercrime incidents at gigantic cost to national economies, corporations and individual digital users; and the emergence of ever more potent internationally operative crime consortia, with readiness and potential to serve as cybercrime or cyber conflict mercenaries. As stated earlier, these developments, taken together, represent a new dimension, if not a quantum leap of the cyber threat, susceptible of undermining cyber confidence even further;
- The persistent uncertainties surrounding Internet Governance, raising concerned questions about the possibilities to maintain a "global, interoperable, resilient, stable, decentralised, secure and interconnected network, available to all"[7];

[6] As of this writing, the ever shorter intervals in which major vulnerabilities are discovered and new threats appear, are illustrated, after the Heartbleed scare in April 2014, by the rapid emergence of the Shellshock virus, described as "deadly serious", and conceivably endangering more than 500 million machines.

[7] NETmundial Multistakeholder Statement of April 24, 2014,

- The increasingly awesome challenge to the enjoyment of human rights on the net, caused by massive government censorship of access and content (cyber repression) in a growing number of countries;
- Perhaps most important, and of burning actuality at this very time, is the emergence of uninhibited, limitless and technically unharnessed intrusion into digital systems via big data search. This has given rise to unprecedented levels of digital industrial espionage and unchecked, often seemingly groundless mass spying by the intelligence services of certain States, reaching beyond their national spheres and unscrupulously impinging on the sovereignty and legal order of other nations[8].

There is no doubt that restoring confidence is a challenge to which all stakeholders in the digital world must respond, and it is hoped that the current publication can contribute to this end, joining other institutions and organizations that pursue the same goal of rebuilding trust in a cooperative, balanced manner[9].

The approach in this book to the task at hand concentrates on three problem areas of immediate relevance to rebuilding cyber confidence, themes also currently under intensive public discussion elsewhere.

In perusing these three chapters the reader should be aware that this publication is not a textbook, a treatise aiming at comprehensive coverage of this complex topic, nor at projecting a single, authoritative position on all aspects of it. Rather, the publication is so structured that it combines various texts written by the ITU, and signed contributions by the members of the World Federation of Scientists expressing their personal views. Beyond the Legal Notice and Disclaimer to be found at the outset of the book, it should be emphasized that the editors have deliberately encouraged a range of perspectives to be presented in order to enrich the debate, while ensuring the overall compatibility of views.

The first part reflects the search for a more comprehensive normative framework to regulate cyber conduct and make it more predictable and calculable. It focuses on

[8] On the importance of trust in this respect, see Leif-Eric Easley, *Spying on Allies,* SURVIVAL, Vol. 56 number 4, August-September 2014, p. 141.

[9] Well-attended recent international conferences also sound the confidence theme, such as the Second Cyber Security Summit, organised by the Munich Security Conference and Deutsche Telekom, Bonn, November 2013, in which Howard A. Schmidt, a contributor to this publication, participated and gave a keynote address.

international efforts aiming at the elaboration, acceptance and practice of confidence-building measures and agreed codes of conduct to enhance trust – as do other, broader legal tools conducive to boosting cyber confidence – in terms of harmonised legal prescription and cooperative international law enforcement. The ambition is to chart the way ahead for gradual, but consistent international and national consensus-building in the normative sphere.

The second part places emphasis on cyber defence and the ability of digital systems to withstand attacks and conflict, and on means to reduce vulnerabilities, mitigate or stultify attacks, or restore the capabilities of systems suffering attack-inflicted damage, or disruption caused by cyber faults, errors and failures. The key term is resilience[10]. After analysing current and anticipated threats, this chapter develops a wide array of techniques and strategies that conjointly may help to tilt the balance towards successful defence in the age old attack versus defence contest so violently being played out before our eyes in today's digital universe.

The final chapter deals with the balance between the freedom of the Internet – and all other digital communications – and government-ordained encroachments: the balance between digital privacy and State security. Is it true that "privacy is dead", given the overwhelming, apparently unlimited technical means of spying on every private and corporate communication and data storage with impunity? This chapter seeks to clarify the extent of legitimate surveillance by foreign and national intelligence services, and the legal basis – especially as it pertains to countries other than those organising the surveillance – for assuming a license of such dimension. It also explores the availability of sanctions against such excessive practices. It hopes thereby to contribute towards the adoption of a binding, concerted framework that balances legitimate security concerns against fundamental rights, the validity of State legislation ensuring data protection and data security, and the basic concept of the freedom of the Internet. This burning issue, like that of illegitimate government censorship of the Internet, needs ample discussion in an international perspective.

And evidently, the overall purpose of this triple discourse is to prevent cyber confidence from eroding further, and to restore it effectively and enduringly. The crisis of cyber confidence must be overcome.

[10] Resilience, the ability to withstand adversity, to persevere and to recover, is more than the conjunction of interacting technical fixes. The term also implies the overall strength – as opposed to fragility - of whole systems over time. See Dhruva Jaishankar, *Resilience and the Future Balance of Power,* Survival, vol. 56, p. 217, June-July 2014.

Chapter I: Cyber Norms

Introduction

This chapter presents an overview of the challenges and current efforts under way to define a set of norms, principles and best practices for cybersecurity at the international level. Emerging threats from espionage to warfare-like attacks and the multi-stakeholder, transnational, and technical nature of the Internet present an unusual field for States in cyberspace: national governments face a domain over which they usually have only tangential control, but in relation to which they are increasingly compelled to protect their citizens, especially as regards their human rights. Some comprehensive regional and a limited number of global efforts are currently being made towards establishing common, basic norms that aim to attain such protection.

Information and communication technologies (ICTs) are increasingly ubiquitous, and their use is growing exponentially in both developed and developing countries. A secure, trustworthy conglomerate of ICTs is a prerequisite for confidence in their expanded use. There are, however, a number of current trends undermining that trust:

- large-scale espionage for national security purposes, facilitated by the sharp decline in the costs of collecting and storing personal information;
- use of computer code for warfare-like actions that transcend national borders;
- a seemingly untameable and eclectic group of rogue actors, ranging from spammers to developers of botnets for hire;
- and difficulties in ensuring the accountability of cyber criminals located in a different jurisdiction to that of the attacked system.

An effective response to these complex issues requires transnational cooperation. This chapter presents efforts in that direction, including notably those undertaken by the United Nations (UN) system and other intergovernmental bodies, as well as some basic recommendations for a global cybersecurity accord. Confidence-building measures (CBMs), a term first used in the Cold War era, are a central element of these initiatives.

The chapter is divided into four sections. First, it highlights the need for the engagement of States in CBMs, the challenges they present as well as their potential benefits. It then discusses the UN approach to norms, rules and principles related to cybersecurity, including principles and recommendations looking forward, and also the applicability of international law to ICTs. The third section describes the latter in more detail, presenting an overview of the similarities between cyberspace and cyber-based actors and actions with other domains of warfare and espionage, as well as a broad set of guidelines for the development of a global treaty-like instrument for cybersecurity. Finally, the fourth section presents the UN vision for cybersecurity, emphasising the established and forthcoming mechanisms of the specialised agencies and a long-term view of the role of the international system regarding cybersecurity and cybercrime.

It would have been tempting – and from many perspectives even appears necessary – to include a further section on Internet Governance, as this book has identified the uncertainties about the future of the Internet as being among the evident causes for the erosion of cyber confidence. Yet, the ongoing international debate on governance where the dividing lines between contrasting government positions still have not been bridged, makes it difficult for the ITU to come down with firm views. It is however possible to note with satisfaction that the deliberations that recently led to the negotiation of the NETmundial Multistakeholder Statement, adopted at the NETmundial conference in Brazil in April of 2014, have produced tangible progress, and that – although the document is deliberately characterized as non-binding – one can observe an incipient worldwide consensus on some of the basic underlying issues. Commensurate with its global calling, the ITU can certainly support all efforts to maintain the Internet as a "global, interoperable, resilient, stable, decentralised, secure and interconnected network, available to all", as a unified, unfragmented space. In the same spirit, it can support the affirmation in the NETmundial conference Statement that "mass and arbitrary surveillance undermines trust in the Internet and trust in the Internet Governance ecosystem".

1.1 The role of CBMs in a renewed vision of international cybersecurity: prospects for a global response and an international treaty

By Solange Ghernaouti

The essential need for cyber confidence

In the space of only a few years the Internet has become omnipresent and virtually indispensable in our daily activities. Nobody can escape the Internet tsunami. With smart devices, more and more services are becoming dematerialised, including those related to health and medicine, the cloud computing paradigm, the Internet of Things that we are heading towards, and the idea of being completely used to being permanently connected and ICT dependent. Nowadays the Internet can be seen as a kind of digital prosthesis and cyberspace as a "natural" extension of our environment. As a factor of change and civilisation, the Internet is structuring the information society that we are in the process of developing on a global scale. It forms part of the continuous process of evolution and human inventions that make up our history.

The adoption of digital technologies has deeply and irreversibly changed our ways of communicating, behaving, thinking, playing, learning, doing business, influencing, destabilising and damaging, and even of monitoring, waging war or policing. The technology is therefore not neutral, as it brings about significant structural changes that affect us directly.

Everyone is using the same Internet, for private, personal and professional applications, for health, energy, supply chains, culture, or even security. Thus, from entertainment to the world of finance, and for all the control systems for vital infrastructure, information and telecommunications, its use has become inescapable.

The Internet and its array of tools have accelerated the technological dependency of both our society and, to an extent, humans. We create and process increasing amounts of information, traffic and interactions. We consume more information, ever more computer resources and energy, with the consequence of creating ever more information waste.

Information technologies have thus become the common denominator for all disciplines and the memory of our heritage (digital cultural heritage, digital heritage of businesses and individuals). There can be no more knowledge or science without information technologies. It should also not be forgotten that the great founding principles of our society, such as democracy, individual identity and State sovereignty, also rely to a certain extent on information technologies – or can be destabilised by their misuse or hijacking.

Let us mention in passing the role that social media and the range of communication tools on the Internet can play in strategies to influence, whether utilised by States, lobbies, or criminal or terrorist groups. Deployed to damage reputations, influence people, crowds and leaders, spread disinformation, and manipulate opinions, the Internet has become a prized information warfare battleground. At the same time, information technology enables the ill-intentioned and criminal organisations to become ever more efficient in giving expression to their limitless and nefarious imaginations and to wage new kinds of war in cyberspace, including information warfare. Refusing to acknowledge this reality is to expose oneself unnecessarily to the potential loss of economic competitiveness, stability, national sovereignty and international credibility. The media, as well as subject matter specialists, report an endless series of cases of businesses having suffered large-scale theft of data, successful cyber attacks, or the seizure of information resources held against ransom.

Confidence cybersecurity has thus become essential, not only in ICT infrastructures, the services offered and the information they process, but also in their security.

Going beyond complexity, cyberspace is changing the concept of territories to be secured

The world today is complex, globalised and above all dominated by the intensive use of ICT devices, infrastructures and services. The dependence on and interdependence and of critical infrastructures and ICT infrastructures have introduced new vulnerabilities for society. This has raised the level of complexity of how we can secure, protect and defend our vital activities carried out at political, economic, societal and individual levels. Also, the interdependence of risks has degraded the overall resilience framework, be it at national or international level. Cybersecurity – regardless of whether we call it that or refer to it as information security or digital security– has become the major issue it is today as the consequence of preoccupations emerging from politics, economics, legal matters, and technologies. Its management is thus crucial, and the various elements involved in seeking solutions for security requirements are complex.

Cyberspace is an area that is both virtual and real, comprising Internet technologies, services and data. It has become – at least for the younger generations – just as much a part of the natural landscape as land, sea, air and space, in the same way as electricity is natural to us. Some view cyberspace as a dynamic territory in constant evolution, or as a territory to conquer, master or control. Yet others see it as a domain where power can be expressed and exerted, or a source of either legal or illegal personal or economic enrichment, or as a citadel of freedom – or as a battlefield. In reality it is to varying degrees and extents a patchwork of all of those things at the same time. Overall it reflects our political, economic and social realities, and is neither better nor worse than them. It bears witness to the reality of the phenomenon of globalisation, of which technical-economic unification is a part.

If in a hyper-connected world the concept of territory is difficult to define, but is even so in relation to the security and defence of digital territories. Traditional ways of thinking of security can no longer apply. Implementing perimeter security to isolate information environments has become impossible as a result of the evolution of technologies (mobile data, smart devices, and the cloud) and their use (social networks, e-payments, etc.). The implementation of cryptographic solutions often acts as a brake on the integration of services, the ease of use, and on providing acceptable performance. Cryptography remains underused and confidence in cryptographic solutions is weak. The “Heartbleed” affair[11] in April 2014 revealed a major bug in the implementation of security in one of the most widely used solutions incorporated into web services. Once again the public was made aware of vulnerabilities in the services supposed to improve the robustness of infrastructures and the security of electronic transactions.

The fragility of confidence

With the Internet, individuals, organisations and States are being confronted by previously unknown cyber threats and new risks. Cyberspace is subject to breakdowns, malfunctions, and cyber criminality, and cyber aggression. Cyber threats are still far too often insufficiently recognised and misunderstood and thus easily create fear. We cannot necessarily predict when or how these threats will become reality, or the domino effects and sequences of events they will provoke, or identify their authors and the people behind them.

As a result most notably of the WikiLeaks (2010)[12] and Prism (2013)[13] affairs, we now know for certain that digital secrecy does not exist, and that we are kept on a close electronic leash and tracked, followed, observed and monitored. We have to recognise that we are being monitored on a very large scale and that we are actively participating in this through our use of certain web services or mobile telephones. We can no longer remain unaware that our personal data, behaviour, tastes and relationships form the basis of the economic models adopted by the majority of the providers of so-called free services and that this information is highly desirable.

Nowadays, the monitoring capabilities of information technologies and their providers are provoking a global crisis of confidence in both these technologies and the main actors in the sector. We are becoming increasingly aware of the fragility of digital environments, the fragility of confidence in technologies and actors in the field of cybersecurity.

Developing confidence in ICT infrastructures requires addressing and overcoming difficulties at a number of levels. These include:

[11] https://www.schneier.com/blog/archives/2014/04/heartbleed.html

[12] http://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points

[13] http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

- The difficulty for individuals, organisations and authorities in understanding threats, identifying risks, and implementing efficient and effective risk-reduction measures, including the difficulty in unblocking sufficient means for combatting cyber criminality.
- The difficulty in preventing cyber abuse and excesses, and in managing the incidents, even crises, that might result.
- The difficulty in protecting citizens, consumers, children, our digital heritage, and our secrets.
- But also the difficulty in expressing our needs for cybersecurity and establishing the rights and duties of actors, and in ensuring they are respected.

Going beyond difficulties and insufficiencies: the identification of real necessities

The cyber world has introduced new vulnerabilities and extended the range of threats that can exploit them. The news reminds us of this every day with information about cases such as data theft, loss of control, information resources being held hostage against ransom, hacked mail accounts, swindles of all kinds, and misplaced trust. Terms such as "hackers" or "Anonymous" or "computer virus" are now commonplace and cyber nuisances have become a reality for all Internet users.

We need to acknowledge:

- the insufficiency of current security measures;
- the insufficiency of the resilience of our infrastructures and of our capacity to manage the complex crises that might arise;
- the insufficiency of the awareness-raising actions undertaken both for the general public and within educational structures, from primary school to university, including lifelong learning, and of research on the development of "national" solutions;
- the insufficiency of cyber-competence and human resources in every domain and every area of activity;
- the insufficiency of the means granted to justice systems and the police to confront the expansion of cyber delinquency and cyber criminality.

We should also emphasise the insufficiency of knowledge and of a cross-disciplinary, global, systematic, and holistic approach to managing cyber risks, as well as the insufficiency of national and international cooperation and collaboration, of judicial assistance, and of partnerships between the public and private sectors, and between the civilian and military domains.

I have introduced the ideas of fragility, difficulty and insufficiency, all of which are correlated with that of complexity. This refers to the complexity of working with political, diplomatic, economic, managerial, judicial, and technological and human dimensions in order to ensure that all cyber risks are contained. We now know that the information society must be built on measures of confidence and security, that surveillance is not synonymous with security, and that security requires reliable monitoring measures that conform to an appropriate legal framework, rather than being imposed by technologies, suppliers, or the strongest actors. Limits should also be defined for technological globalisation and imperialism.

There is a necessity to understand that cyber risks have become a planetary emergency, amplifying all traditional risks linked, for example, to nuclear installations, pollution, or terrorism, and that there is a **necessity** to act in consequence. Essentially, personal and collective will must be engaged and the means developed and made available to tackle the security challenges of the twenty-first century.

There is thus a real urgency to release resources and implement organisational structures and ad hoc procedures at all levels – cantonal, regional, national and international – in order to increase the advantages offered by information technologies and benefit from the new opportunities they provide. In parallel, the downsides must be reduced, most notably to ensure national competitiveness and economic security which we all depend upon for our well-being.

The urgent need for an international instrument

If we consider cyberspace as a fifth common domain, in addition to land, air, the seas and space, then it urgently requires coordination and cooperation among all nations just like the other four.

We are convinced that there is a real and urgent need for an international agreement for a coherent and global approach to deal with cyber insecurity issues. Organisations, businesses and States face significant risks in relation to the inappropriate disclosure, misappropriation and destruction of data and information. Such incidents, when viewed at a macroscopic level, can be regarded as posing a potential threat not just to the competitiveness or reputation of a business, but also to public safety, security or democracy itself at national level.

If we believe that cyberspace can be increasingly considered as a global economic and military battleground, where cyber conflicts reflecting all kinds of political and economic competition can play out, it is time to frame what is acceptable or not on a common and approved basis and to come up with an effective international instrument for controlling this domain. Without a common understanding and international agreements, it will be impossible to develop effective security measures to correctly protect ICT resources (including critical information and vital infrastructures), to fight against cybercrime and to preserve fundamental human rights. This requires a strong commitment among all relevant actors and stakeholders at national and international levels.

National and international strategies should exist not only to respond to cyber attacks – thus defining post-attack reactive measures – but should also consider proactive measures to avoid security breaches and to prevent unsolicited incidents. This could be done, for example, by developing an appropriate cybersecurity culture, by reducing vulnerabilities that could be exploited to attack systems. By taking into consideration in a systemic manner all the factors that can lead, *inter alia,* to deviant behaviours, crisis, acts of retaliation or crimes, and by enhancing complementary and coherent measures in a holistic and global way.

These issues cannot be addressed effectively on a purely local level. In the same way as the Kyoto Protocol[14] is an international agreement linked to the UN Framework Convention on Climate Change, a Global Protocol on Cybersecurity and Cyber Crime should be seen as a truly universal approach to reducing risks and threats in cyberspace. It should provide the essential architecture for setting up effective national and international measures to counter cyber attacks, and should include the clear definition of acceptable and unacceptable behaviours, as well as the necessary control frameworks.

Fostering an international dialogue

By way of background, in May 2007, the ITU launched the Global Cybersecurity Agenda (GCA)[15], a framework for the coordination of an international response to growing challenges to cybersecurity. In order to assist the ITU in developing this strategic proposal, a global High-Level Experts Group (HLEG) was established. HLEG members were nominated by the ITU Secretary-General, with due consideration of both geographical diversity and range of expertise, to ensure multi-stakeholder representation. HLEG is composed of more than one hundred world-renowned specialists, representing expertise across a broad range of backgrounds [16]. These include representatives of ITU administrations, Member States, industry, regional and

[14] http://unfccc.int/essential_background/kyoto_protocol/items/1678.php

[15] http://www.itu.int/osg/csd/cybersecurity/gca/index.html

[16] http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html

international organisations, and research and academic institutions[17]. In November 2008, the *Global Strategic Report*[18] was delivered by ITU[19]. This included strategies in five work areas: legal measures, technical and procedural measures, organisational structures, capacity building, and international cooperation. The GCA provides the essential architecture for developing effective national and international measures to encourage countries to develop national cybersecurity programmes and international cooperation. It should be seen as an important first step towards a global cybersecurity approach. Since then, there has been a great deal of dialogue worldwide on the subject of cybersecurity[20].

The proposal for "A global treaty on cybersecurity and cybercrime: a contribution for peace, justice and security in cyberspace" emerged from a long period of international cooperation[21].

Towards a global instrument to serve the global community

In order to contribute towards meeting the now universal need to manage cyber risks and combat global cyber attacks, cybercrime, and abusive or inappropriate uses of the Internet, we have been drawn towards identifying the need for a renewed vision of international cybersecurity based upon an effective international dialogue and agreements. In doing so, we aim to contribute towards providing a little more peace,

[17] Judge Stein Schjolberg from Norway was the HLEG Chairman and Solange Ghernaouti was co-leader of the working areas on Organisational Structures and Capacity Building respectively

[18] Moreover, in 2008, ITU created the International Multilateral Partnership Against Cyber Threats (IMPACT), an international public-private initiative dedicated to enhancing the global community's capacity to prevent, defend and respond to cyber threats (www.itu.int/osg/csd/cybersecurity/gca/impact_index.html)

[19] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[20] More information can be found in "The baseline review ICT-related process and events, Implications for international and regional security", ICT for Peace Foundation. See:http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security

[21] In 2009 Judge Schjolberg and Prof. S. Ghernaouti published a first proposal for an international treaty in the form of a small book: "A global treaty on cybersecurity and cybercrime: a contribution for peace, justice and security in cyberspace", available at (www.cybercrimedata.net). It was presented during the Internet Governance Forum at Sharm El Sheikh: http://www.intgovforum.org/cms/2009-igf-sharm-el-sheikh. See also Ahmad Kamal, The Law of Cyber-Space. An Invitation to the Table of Negotiation. UNITAR, 2005. Ambassador Kamal was a member of the PMP when he wrote the book, and UNITAR is a UN organ.

justice and security in cyberspace and hence the physical world. This could lead to a Global Treaty, or a set of treaties, related to cyberspace.

Such a global treaty, or set of treaties, on cybersecurity and cybercrime at the level of the UN should be the framework for peace, justice and security in cyberspace, and should facilitate the development of a global strategy to deter cyber threats from any direction. The process of working towards a UN Cyberspace Treaty should help develop a common understanding of all aspects of cybersecurity among countries at various stages of economic development.

All stakeholders need to come to a common understanding of what constitutes cybercrime, cyber terrorism and other forms of cyber threats. This is a prerequisite for developing national and international solutions that harmonise cybersecurity measures. Moreover, a common understanding will also help reduce the divide between the respective perceptions of cybersecurity in developed and developing countries. Because criminal conduct in cyberspace is so global in nature it requires global harmonisation of cybercrime legislation, effective international justice and police cooperation, and a real will to bring this about.

A cyberspace treaty at the level of the UN should establish the principle that serious crimes against peace and security perpetrated via the Internet and cyberspace are crimes under international law, regardless of whether they are punishable under national law. We strongly believe that the most serious crimes in cyberspace should be defined and handled under international law.

Noteworthy at this point is the Council of Europe Convention on Cybercrime (2001), which finally entered into force on 1 July 2004, and which was a historic milestone in the combat against cybercrime[22]. This Convention constitutes only an example of a regional initiative, and many countries preferred to make use of it only as a reference, because it is and always will be a European instrument. In other words, it is necessary, within a global framework at UN level to establish a treaty or set of treaties including the broadly accepted standards and principles in that Convention, but with certain important additional provisions[23]. In fact, as has already been clearly outlined in the ITU-HLEG Global Strategic Report, relevant measures are related to legal, technical

[22] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

[23] A number of countries do not accept some standards and principles, especially the principle in Article 32 of the Convention on cross-border access to stored computer data with consent or where publicly available. Those countries must be respected for their opinions (Source: Chairman's Report HLEG, ITU 2008).

and procedural dimensions that rely upon organisational structures, effective capacities, and international cooperation.

Agreement on a global treaty would be seen as a follow-up to the HLEG reports and a step forward within ITU's GCA initiative that encourages countries to develop national cybersecurity programmes and to promote international cooperation. A global treaty should commit them to doing so.

A vision for the future

Building a secure and reliable cyberspace will require multiple resources and skills. Such a project will be based not only on dedicated technologies and management procedures and a specific legal framework enforceable nationally and compatible at international level, but also on means of governance and control recognised and verifiable internationally.

Certain fundamental principles will also need to be identified, adopted and widely recognised by the international community, following the example of the 1948 Universal Declaration of Human Rights[24].

It will not be a simple matter to define these commonly accepted values, given the differences in countries, cultures, and economic and political interests. Development of a global treaty will doubtless be a long process. This is why it is urgent to initiate a mechanism now to facilitate an international dialogue that will be completed in a time frame commensurate with the urgency of the global stakes in play.

Despite the difficulties involved in coming up with such a treaty and, of course, the probability that it might not always be respected, as my example of the Universal Declaration of Human Rights sadly illustrates, it would nonetheless constitute an instrument to be deployed against bad behaviour, be it by individuals, organisations or States. Moreover, it should help to avoid a drift away from common values, or at least highlight divergences and allow, where appropriate, compensation through legal channels.

A kind of "cyber technology non-proliferation treaty" could prove to be insufficient, however, as it would reduce cyberspace and information technologies to the status of tools of the military world that could be used as weapons. But the frontiers between the military and civilian worlds are not clear; the same technologies are used and the Internet is the same for everyone, from the very youngest to the most senior users.

[24] http://www.un.org/en/documents/udhr/

One might take as an analogy the 1968 Treaty on the Non-Proliferation of Nuclear Weapons[25], the benefits of which are no longer disputed, despite the continued difficulties in its application; this Treaty was of no use in preventing the March 2011 Fukushima nuclear disaster, which was not the result of military action. On the other hand, an organisational structure such as the International Atomic Energy Agency (IAEA) has shown its value in the coordination of the monitoring of the catastrophe and in the creation of the security measures that followed it. Applied to cyberspace, an equivalent structure should exist in order to promote the safe, secure and peaceful public use of information and communication technologies.

This admittedly daring and limited analogy to nuclear weapons and power stations does not of course cover up the need for a global and holistic approach to address cyberspace security problems. These problems justify the adoption of a treaty (or collection of treaties) that recognises both the military and all other relevant dimensions.

Cyberspace is of benefit to all kinds of criminals whose activities, such as money laundering or human trafficking, impact both the military and civilian domains. But even above these specific considerations, is it acceptable that human rights are not respected in cyberspace?

The Internet and cyberspace have become, at a global level, components of the civilisation that we will leave to future generations as part of their heritage. For this reason, it is both our duty and responsibility, individually and collectively, to determine together the common values we wish to promote and see respected internationally, and to implement oversight mechanisms to ensure they are respected.

Confidence-Building Measures

Every actor forming a link in the digital chain, and every country, has a role to play in respect of cybersecurity and cyber confidence. Security is expensive, as are digital insecurity and the absence of confidence. Today, the costs of digital insecurity are essentially borne by users and society in general, partly in respect of the police and justice systems required to combat cybercrime, and partly due to the economic

[25] Treaty on the Non-Proliferation of Nuclear Weapons. Opened for signature at London, Moscow and Washington on 1 July 1968: http://www.un.org/en/disarmament/instruments/npt.shtml
(UNODA United Nations Office for Disarmament Affairs: http://www.un.org/disarmament/
UNIDIR – United Nations Institute for Disarmament Research: http://www.unidir.org/html/en/home.html)

destabilisation caused by cyber attacks, data leaks and cyber espionage. All of these could lead for example to corporate failures, damage to the public image, loss of client confidence, loss of market share, and loss of jobs.

Cyberspace must not be a battlefield or a zone of organised criminality, which is why we must work together to find, honestly and with complete sincerity, the means to develop a trustworthy cyberspace for our and future generations. I am convinced that this will come about through an international treaty, a real Universal Declaration of the Rights of Man (and of Women and Children) in cyberspace. Such a treaty could contribute towards building confidence in cyberspace provided there is willingness and commitment at individual, organisational and State levels worldwide to respect it and to develop practices that take it into account.

While remaining conscious of the limitations of such an undertaking and of yet another international treaty, its main advantage doubtless would be to spread awareness of the needs for security and confidence.

Within an ensemble of confidence-building measures such a treaty, the result of international dialogue, could become:

- A genuine tool for increasing awareness, for communication, and for the promotion of questions of security and peace in cyberspace and in the physical world;
- A reference work that encourages economic and institutional actors (including in the police and judicial domains) to adopt good practices;
- A starting point for developing services and technologies that increase digital confidence and reinforce justice mechanisms and the fight against cybercrime;
- An instrument that assists in ensuring respect for a minimum level of security on the Internet and that reduces the level of cyber violence that populations should need to tolerate.

Conclusion

It is time to act pragmatically to preserve and protect our digital heritage and to make it prosper, to contribute to developing economic security, jobs and competitiveness. These are just a few of the requirements and stakes for citizens, without needing to insist on the respect of their fundamental rights, which are finally the same for security that can be defined, with different levels of importance, for individuals, organisations and States.

Together we will be stronger and will provide cohesion and consistency to our security measures. Digital territories can no longer be protected in isolation because viruses, both biological and electronic, do not recognise national borders. Neither do cyber attacks, which can traverse numerous infrastructures, including those belonging to our traditional allies and neighbours.

Protecting infrastructures, developing resilience, combatting cybercrime, and reinforcing the national stance in respect of cybersecurity and cyber defence are the activities that a well-informed cyber citizen should now be demanding in order to bring about an enduring information society.

Popular wisdom tells us that the roof that protects us from the rain was put in place during good weather: let us then act before it is too late.

It would be naive and dangerous to wait for vulnerabilities to disappear by themselves and for the threats to exploit them to materialise. We need to be proactive and reinforce cybersecurity in order to avoid, among other things, the predation of our information resources, knowledge, intellectual property and personal data, and also to avoid the disproportionate increase in power and hegemony of certain actors, be they legitimate or criminal bodies.

Without wishing to show naivety or excessive paranoia, it is time to integrate into our security strategies the fact that the Internet has changed the ways in which power can be exercised and created new forms of conflicts between individuals, between institutions, and between States.

1.2 UN and Member States' Approach to Internet Norms, Rules and Principles: Evaluation of the Report of the UN Group of Governmental Experts

By Henning Wegener

It clearly emerges from the preceding analyses that international awareness of the need to establish a universal order of cyberspace and, within it, norms for responsible behaviour by State actors and other stakeholders, has been growing in a steady, if not exponential manner. Even If the cyber sphere at its inception was not altogether a lawless space, a void, it certainly has continued to be one that lacks a comprehensive, consensual legal framework not only for States, but for all stakeholders. The perennial task was, and is, to develop over time a convivial behaviour conducive to establishing universal norms. In the performance of this task, and with this very universal perspective in mind, this contribution focuses on recent UN activities, and more specifically on the results of the work of a specialised UN Group of Governmental Experts.

Since then, there have been several highlights over the past few years in an organised worldwide effort towards normatively regulating cyberspace: the series of UN resolutions since 1998; the adoption of the Budapest Convention on Cybercrime as of 2001; the WSIS process; and much purposeful national legislation in terms of civil law regimes that govern torts and damages, penal law, administrative regulations, as well as the pertinent International Private Law. But the consensus view is that the age of systematic and comprehensive cyber diplomacy only commenced around 2008. Since then, there has been a flurry of multinational activities, an almost confounding wealth of initiatives and processes which, conjunctively, are bringing forth evolutive consensus on the normative necessities in a novel fashion. These developments, too numerous to enumerate and analyse in a single effort[26], will hopefully contribute to a process that is “iterative, with each step building on the last.”[27] Many of them employ the useful tools of working out Confidence-Building Measures or Codes of Conduct, negotiating techniques discussed elsewhere in this publication[28].

[26] Instead of providing a complete listing, reference is made to the most relevant of these proceedings and their documents in their respective context infra

[27] Doc. A/68/98, p. 11.

[28] The thinking in terms of codes of conduct and confidence-building measures or, as some prefer, transparency and confidence-building measures, has clearly supplanted the earlier fascination with the concept of a comprehensive Convention on Cyberspace comparable to the 1982 UN Convention on the Law of the Sea. The obstacles to such an instrument and its creation were increasingly recognised as overwhelming. Cyberspace might be even more complex than the ocean world. Digital technologies and their uses are still evolving at a rapid pace. Universal treaty-making would be beset by still bigger cleavages in individual nations’ views. Treaty negotiation would be a lengthy process, and national ratification procedures would not proceed on a time scale even marginally in keeping with the urgency to fill the legal void and the growing, shared perception that the threat of cyber conflict and unmanageable cyber damage is escalating out of control. Thus, while a Universal Treaty/Law on Cyberspace remains a preferred objective, a target concept, an alternative approach is more desirable for practical reasons at this juncture and perhaps for a foreseeable time – an alternative approach is more desirable for practical reasons.

Fortunately, they have already evoked a number of very fine synthetic reports that facilitate an overview and further processing[29].

The biennium 2013-2014 has been particularly fertile in fomenting these developments. It has, apart from many other results, given birth to at least three documents of a seminal nature: The Tallinn Manual on the applicability of international law to cyber conflict[30], the NetMundial document on Internet Governance[31], and especially the Report of the UN Governmental Group of Experts finalised in the summer of 2013 and submitted to the UNGA at its 68th Session [32]. All three landmark documents are discussed in this volume. This article concentrates on the latter report, but also refers to other documents and processes as required.

The 2013 report produced by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security thus the complicated denomination – is not a stand-alone product. The Group's work, and its mandate "[…] to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space, as well as the concepts aimed at strengthening the security of global information and telecommunication systems", takes off from the results of its predecessor, the (2nd) GGE and its report of July 2010 (A/65/201). It also benefits from the trends set in motion by a series of government-sponsored multi-stakeholder conferences from London to Budapest, where the very discussion on norms and confidence building reflected in GGE's mandate took centre stage. The many consultation processes in regional organisations, and in major international organisations like the UNGA, EU, the G8, NATO, and the UN regional organisations also provided intellectual inputs. The

[29] Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas "Baseline Review. ICT-Related Processes and International and regional Security (2011-2013)" www.ict4peace.org, Geneva, March 2014; *Annegret Bendieck, "*Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit", DGAP, Berlin, December 2013. See also *Henning Wegener,* "Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures", Erice, August 2012, available at www.unibw.de/infosecur

[30] "Tallinn Manual on the International Law Applicable to Cyber Warfare".edited by Michael N. Schmitt. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press 2013

[31] NETmundial Multistakeholder Statement, http://netmundial.br

[32] UN document A/68/98

GGE Report therefore reproduces evolving common perspectives, and in some instances emerging consensus. It stands in a continuity of mature reflection about the cyber issues on hand. At the same time, it marks a new step in that problems already under discussion elsewhere are synthesised in a new way, by a representative, quasi-global group of governments. Also, the continuation of the process is assured by the creation of a further (4th) GGE with an even broader, more representative membership of 20 countries ,for further study of the recommendations of the Report (A/RES/68/243), with an enlarged mandate to study "[…] the issues of the use of information and communications technologies in conflict". It is further assured by international follow-up events: in 2015, the Netherlands will host a series of major cyberspace conferences in which individual governments will contribute to promote the evolving consensus further. Already the Seoul Conference on Cyberspace of October 2013, held immediately after publication of the GGE Report, united some 90 governments, and endorsed most of the recommendations of the Report verbatim by consensus in its Seoul Framework for and Commitment to Open and Secure Cyberspace. Although the GGE Report is – like the NETmundial Multistakeholder Statement – "non-binding", it carries a momentum that holds the promise of further stages of global consensus.

The last two chapters of the GGE Report containing recommendations are of central interest here. They include recommendations on norms, rules and principles of responsible behaviour by States, and recommendations on CBMs and the exchange of information. As the role of CBMs in a renewed vision of international cybersecurity is the subject of another contribution to this publication, the discussion of the latter section will be a summary one here.

CBMs, to remind ourselves at least of the gist of them, have the potential to reduce threat, enhance transparency, make State behaviour predictable, are flexible, voluntary, and offer a variable geometry in terms of participants (it is possible to include non-State actors) and follow-up. Contrary to coherent treaty making, participants are free to adopt partial solutions and enact them without delay and independently or with other like-minded stakeholders. CBMs which States embrace do not require ratification; they invite emulation, and are at most – and at best - politically binding. They are thus uniquely suited to foster international consensus-building on an evolutionary scale. A well-negotiated package of CBMs with a critical mass of participants may set in motion a process of further incremental change and heightened sensitivity. Clarification of behavioural standards may provide an incentive to go for more.

The concept of CBMS was pioneered in the former confrontational East-West context in the then CSCE and in the UN, but is now of universal application[33].

The recommendations in the GGE Report centre on international cooperation, transparency, time-critical international information exchanges, early warning procedures around 24/7 approaches and the CERT mechanisms, harmonization of legal prescription, law enforcement, institutionalised dialogue, and other "practical" aspects. To great advantage, they also stress the necessity to involve the private sector and civil society, thus promoting a multi-stakeholder philosophy. They are embedded in catalogues of confidence-building behaviour in part already traditional in other international activities and benefit from such recommendatory packages as the ITU Global Cybersecurity Agenda spelling out global cooperation tasks culminating in "[…] a framework of a global multi-stakeholder strategy for international cooperation" and dialogue.

Many of the measures recommended also take their cue from those introduced by the G8 in 1998, the EU Framework Decision of 2003, or the relevant chapter of the Budapest Convention. Of particular significance is the Initial Set of OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies[34] recently adopted by the OCSE Permanent Council, as that organisation with its comprehensive East-West membership encompasses a broad geographical spread of nations normally displaying different perceptions. From the non-government scene, surely the most complete and systematic analysis of cyber CBMs is the compilation by ICT4Peace, Geneva 2013, based in part on a Zurich conference convened by the same excellent organisation[35].

The Recommendations on norms, rules and principles are perhaps of even higher relevance for a manageable order of cyber space and cybersecurity; they thus deserve a more detailed examination. It will also be necessary to demonstrate the lacunae and

[33] For the earlier development of the concept in Europe and beyond see Henning Wegener "CBMs: European and Global Dimensions" in: F. Stephen Larrabee and Dietrich Stobbe, eds., "Confidence-Building Measures in Europe", Institute for East-West Studies, New York, 1983. The UN-adopted guidelines are reprinted in UN document A/S-15/3. For other applications, see e.g., the Montreux Document on Operations of Private Military and Security Companies During Armed Conflict, www.icrc.org, or the 2010 Draft EU Code of Conduct for Outer Space Activities, http://register.consilium.europa.eu

[34] OSCE Document PC.DEC/1106 of 3 December 2013

[35] "Confidence Building Measures and International Cyber Security", www.ict4peace.org

ambiguities of the text, and, proceeding from a first analysis, to point to the assignments still pending and the inherent challenges to the 4th UN GGE in its now incipient work - and to other cybersecurity frameworks.

The significance of the brief catalogue of essential norms and principles derives in good measure from the fact that government representatives from the five Permanent Members of the UN Security Council as well as from India and Japan also joined in the consensus. Notwithstanding its non-binding nature it is thus an authoritative reference.

In many quarters, it has been emphasised that the Group's conclusion that international law and especially the UN Charter are fully applicable to the use of ICTs is of particular significance. This principle has been advanced before in several international documents, but has never been so unequivocally stated. This constitutes important progress, even though it is immediately conditioned by two other sentences noting that how these norms apply to State behaviour requires further study, and that additional norms geared to the unique attributes of ICTs could be developed in future.

These caveats reflect well-known and lasting differences in the perspectives on global ICT management among some of the major countries, and have required a balancing act throughout the drafting of the Report. The paragraph on the applicability of international law is thus immediately followed by one affirming the applicability of State sovereignty to ICT-related activities and infrastructures within State jurisdiction.

The reaffirmation of the validity of international law in cyberspace includes, as spelled out in a further paragraph, the respect for human rights and fundamental freedoms under the relevant international conventions, a principle - even if already underlined in many other international documents from the WSIS onwards - surely of great importance for the future of Internet freedom and the fight against government Internet censorship.

The applicability of the UN Charter also extends its basic provisions on the maintenance of international peace and security, the command to refrain from the threat and use of force, and the right to self-defence against armed attack to the cyber realm. However, pending "further study", the Report does not address the question of hostile use of ICTs. While certainly aware of the draft international code of conduct for information security submitted in 2011 by Russia, China and others[36] – a document expressly cited in its chapter on recommendations on norms – the Group did not

[36] A/66/359

include an equivalent to the earlier draft's following norm: "Not to use information and communication technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies" – a regrettable omission from this author's perspective. However, the remainder of the norms and principles spelled out are certainly worthy of acclaim and appear in principle uncontroversial. That holds particularly for the recommendations on enhanced cooperation against criminal or terrorist use of ICTs, the harmonisation of legal approaches, and collaboration in law enforcement and between prosecutorial agencies.

Not less meritorious is the list of norms/principles laid down in paragraph 23 of the Report: States are to meet their international obligations regarding internationally wrongful acts attributable to them – however difficult the attribution of cyber abuses; they must not use proxies to commit internationally wrongful acts; and are to "seek to ensure" that their territories are not used by non-State cyber criminals. The binding adoption and translation into national legislation of these norms by a great number of countries could form more efficient instruments to counter the activities of botnet operators and cybercrime consortia. Moreover, international pressure could hopefully unfold to ensure application of the necessary national law enforcement measures.

Finally, the text incorporates a normative reference to the private sector and civil society to help improve cybersecurity including more secure ICT uses such as "supply chain security for ICT products and services." This is a reminder that cybersecurity is a societal task requiring multi-stakeholder participation and responsibilities that have to go beyond "responsible behaviour by States."

Taken together, the various sections of the Report – apart from the norms/principles part and the CBM chapter there is also one on capacity-building measures with useful, although less exciting recommendations – constitute indubitable progress. The Report does not eliminate, but certainly mitigates some of the important fundamental cleavages in nations' views on the future management of the cyber world. The remaining differences in basic philosophy pose a formidable challenge, especially when the next GGE will "study further" the incipient broad consensus and set about working out detailed prescription.

Yet, the Report, following as it does the series of major international conferences (London, Budapest, Seoul, etc.) and the work of regional international organisations, has now consecrated the double approach of designing CBMs and elaborating the norms and principles for a code – or codes – of cyber conduct. Whatever future negotiating formats are adopted, this approach will make State behaviour more predictable, is flexible, voluntary, and offers variable geometry in terms of participants, State and non-State, and follow-up: contrary to coherent treaty-making, participants would be free to adopt partial solutions and enact them without delay and independently or with other like-minded stakeholders. Yet, the consensus reached by the GGE is only partial, and the challenges faced by its successor GGE will be daunting.

The Group constituted itself in late July 2014, elected its member from Brazil as Chairman, and agreed its working calendar, and a division of labour among the 20 government Experts. These are now to prepare, or revise their position papers and contributing drafts accordingly. The Group will meet again in January 2015 with a view to reporting out by the summer of that year.

Among the primary, and most complex tasks of the GGE will be the more detailed definition of international legal rules pertaining to international security and peace, including the definition of what constitutes an "armed attack" in cyber terms; what sovereignty constitutes in the cyber age; how hostile uses of cyber technology (”cyber weapons", including malware dedicated to attack and damage military and infrastructure assets) can be restrained and embedded in a regulatory framework. These issues have been with us since the inception of the cyber age, but become more worrisome as unbridled cyber armament by a growing number of States is part of present-day reality, especially as no legal or political limits are in sight in these often-misguided efforts.

The Tallinn Manual – to be discussed elsewhere in this publication – no doubt offers valuable insights and guidelines for analogies from conventional international law, but is, without doubt, a product from a predominantly "Western" group of legal experts that need to be checked against more global perspectives. A critical appraisal of the Manual also shows that an analysis basically taking the law of armed conflict as a starting point tends to accept hostile or military use of cyber technology as a regular option – "one of those things" – even though the limits and modalities of potential use are more or less clearly spelled out by the Manual authors. Not surprisingly, the Manual, despite its prudence and careful wording, has been interpreted in many quarters as an "invitation to cyberwar." Surely, an overriding caveat highlighting the basic inadmissibility and inherent dangers of cyberwar would have been apposite.

A further challenge lies in the – necessarily – general nature of the Report's recommendations. In each case, translating them into practice and filling out the general prescription in detail will be extremely difficult, all the more so as the inclusion of the various regional processes and of a broad multi-stakeholder community need to be managed with a view to reaching compatible outcomes.

Under these circumstances, designing a forum – or fora – where intensive talks and later negotiations can be launched is a complex task. The GGE Report recommends regular institutional dialogue with broad participation under UN auspices as well as regular dialogue through bilateral, regional and multilateral forums, and other international organisations. This certainly goes in the right direction, but is too unspecific for allowing rapid decision making on the procedural way ahead. It would probably be wise to narrow the institutional choices by first agreeing on the criteria a forum should meet (inclusiveness and openness, allowing a broad stakeholder community to participate in full, support by an experienced international secretariat with ICT expertise, etc.). A single forum offering a universal perspective would certainly be the most desirable course. On the other hand, preliminary regional endeavours are already under way, and their dynamics should be used. An autonomous conference of States able to establish its own rules of procedure and modalities of broad stakeholder participation could perhaps be considered an adequate venue.

Returning to the chapter of the Report offering recommendations for norms, rules and principles, one should with all respect for the work of the authors be reminded that their catalogue, given the political texture of the UN context, and the need to arrive at consensus within a limited time frame, is selective to the point of being incomplete. Surely, the forthcoming 4th GGE should take a close look at additional norms and principles proffered in recent times[37].

More explicit norm setting is particularly necessary in the core areas of security, cyber stability and cyber peace[38]. The lacunae to be filled would appear to be, for instance, the following: a call for binding agreement on the fundamental principle that a cyber attack against another State, direct or through hired perpetrators, constitutes a violation of international law; a commitment by all States not to practice first use of cyber weapons against another State, as long as it has not undergone an attack by conventional weapons. States should also subscribe, nationally and internationally, to a policy of cyber conflict prevention, placing the emphasis on cyber defence, restraining and delegitimising the development, use and export of offensive cyber means, especially dedicated attack software. Critical infrastructures should be protected beyond the suggestion in paragraph 26 (e) to increase international

[37] In addition to the work of the regional organisations enumerated in part in paragraph 27 of the GGE Report, see the earlier reference to the work of ICT4Peace, above fn. 6; the article by Henning Wegener, above fn.3; the ITU Secretary-General's five principles for cyber peace, reprinted in The Erice Declaration on *Principles for Cyber Stability and Cyber Peace* 2009, reprinted, in *The Quest for Cyber Peace*, p. 110.

[38] The mandate of the now constituted 4th GGE places emphasis on "conflict" scenarios.

cooperation, by the principle that States are responsible for the protection of critical infrastructures on their national territory and that attacks on these infrastructures are prohibited, thus ensuring also the inviolability of transnational digital net structures. A principle as yet missing is also that States have the duty to protect their citizens in cyberspace. Going beyond the recommendation in paragraph 23, it should be spelled out that the use of botnets and other irregular cybercrime/war practices is forbidden, and that States are obliged to implement this prohibition on their national territory. Finally, neutrality continues to be valid in the cyber age, and cyber attacks - even in self-defence - must not be perpetrated through the net structures of neutral States.

1.3 Does International Law Apply to Cyberspace?

By Gábor Iklódy

The digital age offers tremendous benefits but also multiple threats that can cause major disruptions and even destruction. The fundamental challenge before us is to find ways to protect cyberspace as a trusted environment where we can navigate freely and use its potential fully - but do so in a more "security-conscious" fashion. This requires us to find a proper balance between freedom and security. Neither ignoring the security risks nor using them as a pretext to restrict freedom and civil liberties would help. In order for trust to prevail, it is important to ensure that government agencies fully respect the requirements of democratic accountability in their efforts to prevent malicious activities in cyberspace.

Trust is critical for citizens and not less so for States in their international relations, which is the focus of this paper. What we see today is a sort of cyber "Cold War" being waged with increased levels of cyber espionage and heavy investments, primarily on the part of advanced and resourceful countries in offensive cyber capabilities.

From the perspective of any modern military, it is essential to ensure that its ability to manoeuvre freely in cyberspace is not impaired. This requirement is clearly reflected in an increasing number of national defence strategies, which recognise cyberspace as "a new domain of warfare that has become as critical to military operations as land, sea, and space"[39]. The conclusion is quite clear: cyberspace has become part of modern warfare, and there will likely be no larger scale conflicts fought without a

[39] NATO Policy on Cyber Defence, Brussels, 8 June 2010

significant cyber component. The experience of the past years has provided sufficient evidence on this.

In order for cyberspace to become and remain a trusted domain, a cooperative environment is called for - where certain, commonly accepted rules apply. International norms governing the behaviour of States are essential ingredients of such an environment. But, despite their obvious relevance, it should be stressed that they are far from being the only ones. Cyberspace is a singular domain with a multi-stakeholder character where governments are but one of the players shaping its environment. The need to develop and maintain a genuine public-private partnership in cyberspace is more imperative than in any other domain. "It is the private sector that owns and operates most cyber infrastructure and it is this sector that produces the technology we all need. The private sector represents the first line of defence and private companies and science design the future technological environment governments too will operate in."[40] This does not of course diminish governments' underlying responsibilities arising from what sovereignty entails, and from which they cannot run away.

Today, there are no treaty provisions or customary norms specifically dealing with cyberspace. But does this mean that cyberspace is to be regarded as a grossly unregulated domain, a sort of Wild West, where no norms apply at all? Is the assertion indeed justified that a legally binding set of norms must be urgently elaborated - and is that feasible? Or should the point of departure rather be as UK Foreign Secretary William Hague put it: "Behaviour that is unacceptable offline is also unacceptable online, whether it is carried out by individuals or by governments[41]. "

Applicability of international law in cyberspace

The discussion among experts has been ongoing for quite a while on whether existing international instruments elaborated for the traditional domains are also applicable to cyberspace. The debate slowed down somewhat after 9/11 when the emphasis was placed more on the War on Terror, but it picked up speed again around 2007-08. The focus on terrorism brought many relevant aspects into this revived cyber debate, to include questions like: "How do we attribute the action of non-State actors to a State?"; "What are the responsibilities of a State regarding the activities of such

[40] Gabor Iklody: Speech at the *NATO Information Assurance Symposium*, 11 September 2012, Mons

[41] UK Foreign Secretary William Hague's speech on 11 November 2011 at the first *Cyberspace Conference* in London.

groups operating on its territory and launching attacks against assets in another State?"; "How do we use force legally against non-State actors residing in a different State?"; or "Can one use force to pre-empt a potentially devastating attack and, if so, under what conditions?". All these questions are also very topical in the cyber environment.

To elaborate a global, legally binding arrangement that would establish the most important norms to be followed in cyberspace and describe the consequences of non-compliance may sound tempting. But at present, this does not seem to belong to the realm of what is possible, or indeed even required. The reasons are manifold. First, the domain is evolving so rapidly that it would be virtually impossible to agree on a comprehensive and durable set of cyber-specific norms. Second, national views are clearly far apart on a number of critical issues with practical consequences, such as thresholds, responses and enforcement. Therefore, trying to cast in stone what we think of cyberspace today and - just as importantly - on what we could possibly agree on would force upon us a straight-jacket that may in fact turn out to be counterproductive (particularly in countries with a more legalistic culture). Third, the value of legal obligations that are virtually impossible to verify is questionable.

As experience in other fields including arms control and nuclear disarmament has shown, if mistrust is running high among the parties it is more conducive to results to opt for smaller steps that can first build and consolidate confidence gradually, brick-by-brick rather than put the bar too high and try to force ourselves through apparent difficulties. The experience gained in nuclear arms control taught some very important lessons for us in that regard. Measures that keep communication lines open, offer a degree of transparency and help diffuse tension in times of crisis could help achieve that objective. Bilateral and regional initiatives such as the work of the OSCE on cyber confidence and security-building measures, point in the right direction, but also reflect how difficult it is to come to an agreement, even if the measures proposed are at the low end of the spectrum and are voluntary in nature.

This does not mean that it would be too early to explore international talks and cooperation already now. In addition to CBMs that can help create the necessary environment for more stringent measures there are areas where work could be launched relatively easily. As Joe Nye suggests: "The most promising areas for international cooperation are not bilateral conflicts, but problems posed by third parties, such as criminals and terrorists"[42]. Over time the interests of advanced (and

[42] Joseph S. Nye: "Nuclear Lessons for Cyber Security" in *Strategic Studies Quarterly*, Winter, 2011.

therefore also more vulnerable) States will likely converge in limiting the damage caused by criminal and terrorist groups, which in turn will open the way for them to cooperate on forensics and controls. “States might start with acceptance of responsibility for attacks that traverse their territory, and a duty to cooperate on forensics, information and remedial measures[43].”

With regard to international norms, the way ahead is clearly to accept the relevant existing legal instruments as the baseline, both with regard to *jus ad bellum* (law governing the resort to force) and *jus in bello* (law regulating the conduct of armed conflict), and to apply them to the cyber domain as well. Such a general agreement would allow us to then move ahead and assess one by one which provisions of the existing legal instruments require common interpretation and which ones need to be complemented.

Over the past almost two years, two important international attempts were made to promote a common understanding with regard to the core aspects of the issue, i.e. to cyber attacks. Both the Tallinn Manual produced by a group of independent international law scholars and practitioners under the aegis of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and the recommendations prepared by the UN Group of Government Experts (UNGGE) in the field of IT affirmed that existing international law does indeed apply also to cyberspace. Consequently, the question should not be whether the existing laws apply but rather how they do so. Admittedly, the two groups’ conclusions are not binding, nor have they been agreed by States – at least not yet. Nonetheless, the agreement reached among experts is rightly called a landmark consensus.

The Tallinn Manual[44], is a quite elaborate and ambitious piece of academic study, written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). It examines comprehensively the extent to which legal norms may apply to cyber warfare. It reflects the views of those independent experts who participated in the work of the Group, and no more than that. It is best seen as a genuine effort on the part of the Group to launch a thinking process about a highly sensitive and important set of issues. In other words, it is an invitation to others to be part of a thinking process, and the beginning rather than the end of an effort to build a widely shared, common understanding.

[43] Eneken Tikk: “Ten Rules of Security”, *Survival*, June-July 2011.

[44] Tallinn Manual on International Law Applicable to Cyber Warfare.

What constitutes "use of force" or "armed attack" in cyberspace?

We have a fairly good understanding of what an act of war looks like, but what amounts to "use of force" or an "armed attack" in legal terms in the cyber domain? Can a non-kinetic action – which cyber attack is – be an "armed attack", or only in the event it forms part of a broader kinetic operation? What kind of response to a cyber attack can be regarded as legitimate, and would that include the right to use military force in response?

The term "cyber war" has no universally agreed definition. It is generally used to describe hostile actions in cyberspace "[…] that have effects that amplify or are equivalent to major kinetic violence"[45]. It is therefore not merely the deployment of offensive cyber means but rather the effects of their use that can help us determine whether a cyber war is at play. To date, no one has seen a cyber war in the strict sense of the term. We have seen massive denial-of-service attacks targeting a country or its critical infrastructure as a separate attack or as part of a larger, kinetic offensive, and we have seen targeted attacks against industrial control systems. "But problems of unintended consequences and cascading effects have not been experienced, […therefore] the full set of actions and reactions in a cyber war between states have not been tested"[46].

The UN Charter makes only two exceptions to the general prohibition on the use of force: one is under Chapter VII, in cases when the Security Council determines the existence of a threat to peace and is allowed to take whatever action it deems necessary to restore it; the other is Article 51 when a country exercises its right to self-defence, which at the higher end of the spectrum acknowledges its inherent right to use force against the aggressor unilaterally or collectively.

A few general observations are called for here. To come to an agreement within the UN Security Council on authorisation of use of force often proves difficult. This is largely due to the requirement of "Great Power" unanimity or, in other words, the veto power of the Security Council Permanent Members. Unanimity is at times difficult to achieve, especially in cases when one or more of the Permanent Members are a party to the conflict in question. This, apart from being a challenge to the democratic nature of the process, by implication carries the risk that countries opt for categorising a use of force incident to one of armed attack - which in turn provides them with

[45] Joseph S. Nye, Ibid

[46] Ibid

justification to use force against the aggressor. Another phenomenon that further reinforces the shift toward an expanded application of Article 51 is the emerging right of States to self-defence against terrorist attacks.

What happens when the attacker is not a State but a non-State actor or appears to be one? The UN Charter framers left the concept of "armed attack" deliberately open to the interpretation of its organs and Member States. Also, the wording of Article 51 is broad enough to allow States under attack to exercise self-defence even if they originate from non-State actors. The response to the 9/11 attacks serves as an important example, both in terms of UN Security Council decision making and NATO operational decisions.

But can non-kinetic cyber operations constitute a "use of force" and even amount to an "armed attack" or, following the logic of the UN Charter framers apply solely to the use of military force? Many attempts have been made over the years to clarify whether political and economic coercion could amount to use of force. They have mostly failed as many feared that recognising non-kinetic, non-forceful acts as possible triggers to use force in response would just open a Pandora's Box. But is it indeed right to keep the focus solely on the instruments used or, instead, should one give more attention and weight to the consequences caused?

What matters historically to governments is probably less what specific instruments were employed in a given event but rather what the consequences of their deployment were. Let us recall the 9/11 attacks, when civilian airliners were used to deliberately cause maximum damage and kill people. So here is what could be the rule of thumb: if cyber attacks lead to devastating consequences that are comparable to those caused by kinetic activity, then a cyber attack should be considered as use of force and even an armed attack just as much as a military offensive. From this perspective, it does not really matter whether the attack comes from the air, land, sea or cyberspace; it is the impact of the attack that will increasingly determine how it will be viewed and grant the right to the nation attacked to act in self-defence. Another example could be Syria. The release of lethal chemical substances is generally classified as non-kinetic. But their use in Syria against the local population causing death and injury on a massive scale could probably qualify as use of force.

What happened to the Saudi Aramco oil company in 2012 is a more difficult case. While the complete erasure of all data stored on the company's 30,000+ computers was no doubt an extremely painful blow, and caused a situation that was difficult and expensive to at least partly remedy, many experts caution against calling it an armed attack, with all the ensuing consequences.

So, how to determine whether an event has crossed the "use of force" threshold, potentially also amounting to an "armed attack"? How much damage, pain and fear would need to result before one concludes that a response should be mounted?

Unfortunately, there is no clear-cut answer to this question. The general consideration cited above nonetheless holds true. Namely, if the consequences of the attack are as grave as those of a conventional attack, it could be considered as a use of force[47]. There is an obvious linkage therefore to the severity of the damage, and the number of casualties resulting from the attack. Events that result in a large number of casualties certainly fall in that category, while attacks that paralyse key sectors of life in a country most probably do as well. But can one establish a threshold for that? The answer is clearly no. The decision to call it a "use of force" or "armed attack" event will always remain ad hoc and will take into consideration a large variety of factors. From that perspective, the judgement on what amounts to an act of war is more a matter of political judgement than a military or legal one. It can hardly be any more concrete. Even in the area of terrorism, after the horrors of 9/11 one could not be more specific. Could we for instance conclude that if a terrorist attack targets innocent civilians and the death toll exceeds 3,000 it is then unquestionably an armed attack? Do we want to imply by this that if casualties are kept below the 3,000 threshold then the attack is not to be considered an armed attack? Apart from any other consideration, is this the sort of message one wants to convey to potential perpetrators? I am sure it is not the intention.

Cyber operations can be categorised in a variety of different ways. One generally accepted model is the CIA Triad (confidentiality, integrity and availability) developed to identify problem areas and solutions for information technology[48]. Attacks on integrity, designed specifically to sabotage the normal functioning of control systems (like for instance the Stuxnet virus), or attacks on availability (shutting down air traffic control or blinding military networks, like in Georgia) may cause casualties and their impact may be comparable to that of a kinetic attack. Therefore, they can cross the use of force threshold relatively easily. On the other hand, attacks on confidentiality (espionage through cyber means) can result in huge losses (in the US alone intellectual property theft is estimated at around 250bn USD per year), but they fall in a different category and the answer to them is mainly diplomatic.

[47] See the so-called Schmitt criteria, a set of rules that can help a State decide whether cyber attack is or is not an act of war.

[48] See Darril Gibson's "Understanding The Security Triad", *Pearson*, 27 May 2011.

Espionage, being the second oldest profession, is practiced widely – sometimes even among the closest allies. "At the macro view, every state must balance the, at times, conflicting goals of maximizing freedom of action and minimizing harm. Surveillance of malicious behaviour has the overall goal of minimizing harm, i.e. finding out about threats early enough to allow for disruption to take place"[49]. In an era when prevention and early detection of hostile intent and malicious activity is becoming ever more important in order to prevent incidents rather than trying to deal with their consequences, intelligence is gaining more prominence. To outlaw cyber intelligence altogether in international relations would therefore hardly be a realistic objective. It is however "[…] plausible to imagine a process of iterations (tit-for-tat) which develops rules of the road that could limit damage in practical terms".[50]

The interest to lower the bar of use of force as a means to contain the expansion of espionage is, at the same time, very much present in the thinking of a number of countries, in particular among the less developed ones. The picture is more colourful in the case of the more advanced countries. They are very often the prime targets of such espionage attacks, On the other hand they are the countries most interested in retaining larger room for manoeuvre, and thus are generally not in favour of lowering the bar. As countries wanting greater freedom of action to retaliate as well as possessing the necessary capabilities to do so, they are also more interested in general in reducing the gap between the "use of force" and the "armed attack" thresholds.

Response to a cyber attack

If a country comes under heavy cyber attack, the most important immediate objective is to stop and repel the attack, and reconstitute the damaged systems as quickly as possible. Protection of the population and recovery of critical digital networks are therefore the priorities. In most cases, the goal is to avoid further escalation of the conflict unless the use of force is considered necessary to deter and prevent further attacks.

A major cyber attack involving for example malware knocking out air traffic control, causing planes to collide or crash to the ground and a high casualty toll, would probably be regarded as an armed attack requiring proper response. But even then, under international humanitarian law, the response must meet certain important criteria. It should be proportionate, justified and necessary and should follow the

[49] Interview with Kah-Kin Ho, Head of Cyber Security at CISCO.

[50] Joseph S. Nye, Ibid

principles of distinction and feasible precaution of attacks. As for its content, the response could take any number of forms. It might be a military or a cyber response, or one that names and shames the attacker before the UN, or a diplomatic response, or one that imposes sanctions. And then again, there might be no response at all.

Exercises mimicking real-life scenarios have clearly demonstrated that massive and concentrated cyber attacks launched by capable and resourceful adversaries determined to inflict serious damage cannot be stopped by cyber means alone. If cyber attacks form part of a larger offensive campaign, this is even more obvious. While defensive cyber measures can help restore damaged networks and assist forensics or early detection, they cannot dispel the threat. That requires resort to other measures in a country's toolbox.

Pre-emptive action

Another interesting dimension of the issue is linked to the specificities of cyberspace, namely that the time and space factors largely lose their relevance: there is little or no warning time at all. The time between a computer detecting that it is about to be attacked by hostile malware and a pre-emptive step to disarm the attack may be just a few milliseconds. Effective defence therefore presupposes automated responses, which in itself presents a number of difficult questions. Given the speed of attack, the question is whether a State should wait until a massive cyber attack – analogous to an armed attack – occurs (as a stand-alone action targeting its critical infrastructure or as an integral part of a kinetic operation, aimed at knocking out vital command and control centres), or should it be allowed to respond pre-emptively. If so, at what point should governments step in to prevent destructive cyber attacks – what are the conditions of anticipatory self-defence?

Many legal experts seem to have settled upon a standard known as the "last feasible window of opportunity", where a failure to act at that moment would risk the severe impairment of effective defence. The Tallinn Manual concludes that a State may act in self-defence "[…] when the attacker is clearly committed to launching an armed attack and the victim-State will lose its opportunity to effectively defend itself unless it acts"[51].

Sometimes the use of cyber means is regarded as an alternative to something worse. Advanced and powerful countries may feel tempted to move toward a greater strategic use of cyber weapons to persuade adversaries to change their behaviour or

[51] Tallinn Manual on the International Law Applicable to Cyber Warfare.

stop certain dangerous activities. This can be good, if it averts war. On the other hand, it could cause other nations to feel vulnerable, at the mercy of others, more advanced actors. The fear that it could unleash an even more widespread cyber arms race as nations try to catch up or contract cyber mercenaries is not entirely unfounded. Also troubling is that the code sophisticated cyber attacks have used often becomes accessible on the Internet to non-State actors.

What is the level of proof required for attribution?

Attributing a cyber attack to the perpetrator with a sufficient degree of certainty is often cited as a major problem, one that in fact makes the qualification of a cyber operation as an "armed attack" virtually impossible. No doubt, the problem is real and it would be a mistake to ignore it. But similarly, it should not be over-emphasised either. A more cooperative international environment, better interaction between intelligence and cyber technical communities, and, last but not least, the evolution of technology could all help improve the situation.

If indeed the requirement is to provide clear and compelling evidence linking the attack to the perpetrator in ways that could stand before the court, then indeed the problem of attribution is immensely difficult. But attribution is a relative term. One should accept the fact that, in the event of a cyber attack, finding "the smoking gun" is virtually impossible. Full, absolute certainty can seldom be established even weeks after the attack, if at all. Reliance on mounting evidence collected from a variety of areas (intelligence, technical, etc.) is a more realistic expectation (i.e. the existence of "circumstantial evidence"). Attribution is also a relative term in Realpolitik. Concerns associated with the difficulties to attribute an attack to a perpetrator are commensurate with the number of casualties. In other words, the higher the death toll, the greater the pressure is on governments to respond resolutely to the attack.

It is also important to stress that attribution is not a requirement to qualify an action as an armed attack. Let us remember NATO's response to 9/11, when within 24 hours the Alliance invoked for the first time in its history the Article 5 collective defence mechanism. The formulation employed then by NATO did not make reference to the attributability of the terrorist act to a State. It merely inquired whether the attack against the US was directed from abroad – a requirement to ascertain that the collective defence clause is not used against its own citizens. It is often concluded that deterrence does not work in cyberspace because of the problem of attribution. No doubt, this is partly true – albeit not in the traditional sense when it suffices to put force on display to deter the potential aggressor. But deterrence does work in situations when it can deny the benefit of the attack rather than trying to impose costs through retaliation – precisely as ballistic missile defence renders the attack ineffective or too costly. “If firewalls are strong, or the prospect of a self-enforcing response seems possible, attacks become less attractive”[52].

Non-State actors

In the cyber domain, most intelligence assessments agree that only a limited number of nation States currently possess the capability to carry out complex and sustained attacks causing serious damage. At the same time, as Deputy Defence Secretary Lynn argues, […] “while States have the greatest capabilities, non-State actors are more likely to initiate a catastrophic attack”[53].

Here, I want to stop for a moment and make a clear-cut distinction between espionage, on the one hand, and devastating disruption and destruction on the other - even if technically they are in fact very close to one another. While unquestionably every effort should be made to make espionage and the theft of valuable government and industry information more difficult, eliminating the risk of attacks causing massive devastation is the inescapable priority.

The good news is that, as in the area of nuclear posture, capable nation States think mostly in rational terms and will probably strive to refrain from crossing critical red lines provoking tough reactions. In order for countries to understand this situation they should first know that a red line has indeed been drawn. The message should therefore be conveyed loud and clear: a devastating attack may trigger national or collective counter-measures where anything in the toolbox might be used[54]. Second, there is scope for gradually developing some confidence-building, de-escalation measures, some basic rules, as referred to earlier – again drawing on experience gained in the nuclear field.

It is more difficult to expect rational thinking though from some of the “rogue States” that have the ambition to build offensive cyber capabilities and are investing heavily in acquiring them. They are more difficult to deter and - as some analysts in some of the volatile regions remind us - for certain countries and cultures a “lose-lose” scenario is, at times, an entirely acceptable option.

[52] Joseph S. Nye, Ibid

[53] Deputy Defense Secretary Lynn *Remarks at the 28th Annual International Workshop on Global Security*, Paris, 16 June 2011.

[54] Gabor Iklody speech at the AFCEA Global Intelligence Forum, Brussels 10-11 December 2013.

The biggest worry however is linked prospectively to non-state actors. The ultimate nightmare arrives when the capacity to do harm comes together with the intent to do harm, whatever the cost. We are not there yet, but the fear of terrorists using cyber weapons does not belong to the realm of the impossible. There are “ready-to-use” kits available on the internet that can be further developed, there are 0-day black markets and there are cyber mercenaries, very capable “hackers for hire” groups whose services can be bought to steal money or industrial secrets or, using practically the same tools and techniques, cause massive disruptions.

1.4 United Nations Vision on Cybersecurity

By Hamadoun I. Touré

This section presents the foundations for a UN vision on cybersecurity. ICTs play a central role in present-day development, and the security of those systems is becoming increasingly critical. Developed economies are extensively reliant on ICTs, including for essential infrastructure, making cybersecurity a pressing priority that many countries recognise already. There is a unique opportunity for developing countries to build information infrastructure that is inherently secure, and thus make a quantum leap in their development.

However, cybersecurity is far from being an established global priority, and is often not mentioned in national ICT and development strategies. Through the incorporation of cybersecurity in development programmes, and seeing it as a “means to an end” rather than an end in itself, the UN is trying to change that landscape. This article focuses on the current global need for cybersecurity, the UN vision for its development, the relevant mechanisms now in place, and briefly outlines ongoing or planned cybersecurity initiatives.

The Need for Global Cybersecurity

ICTs have “transformative powers”[55] that have permeated virtually every industry in developed countries, and led fast transformations in developing ones. Ubiquitous computer networks, however, come at a cost – that of making entire economic sectors

[55] Speech by ITU Secretary-General Hamadoun I. Touré, - Transform Africa Summit." International Telecommunication Union. 28 Oct. 2013. Web. 24 July 2014.

more vulnerable to cyber attacks. The scope of these threats is wide, ranging from petty crime to stealing a single credit card number to global, coordinated attacks (e.g., Conficker). Perpetrators of crime often operate anonymously[56], creating additional complications for prosecution. Furthermore, traditional law enforcement units are challenged with limited resources in the cyber domain, and with attackers that often operate from a different jurisdiction. These factors are at interplay in a complex domain that presents both technical and policy challenges to all countries: it is imperative to protect the integrity, confidentiality and availability of both critical information and personal data.

Several developed countries have adopted cybersecurity as a national priority[57]. Confronted by a network that was designed for openness, and not security, countries are spending vast resources to secure their networks, up to an estimate of over USD 70 billion in 2014[58]. However, these expenditures are overwhelmingly concentrated in high-income countries, and they seem insufficient considering that attackers are constantly targeting new industries[59].

Driven by a wide range of motives ranging from financial gain to political activism, cyber threats can emanate from virtually all countries, and affect vast sectors of the economy. No single entity – or State – can deal with them in an effective manner. These factors increase the urgency of a global, concerted effort on cybersecurity.

There is also another, more comprehensive need for cybersecurity that goes beyond the inveterate lexicon of “cyber weapons” and “cyber attacks”. A holistic approach would protect both the right to information and the right to privacy in cyberspace, both of which are fundamental human rights recognised by international treaties. Therefore, in addition to boosting economic development, increasing trust in this new domain by making it more secure would lead to an environment that protects individuals from unauthorised intrusions into their information. It is for all these reasons that the international community should step up efforts to make cybersecurity a global priority.

[56] Nazli Choucri, Stuart Madnick & Jeremy Ferwerda, Information Technology for Development (2013): “Institutions for Cyber Security: International Responses and Global Imperatives, Information Technology for Development,” DOI: 10.1080/02681102.2013.836699

[57] “Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy.” *Organization for Economic Cooperation and Development,* 2012.

[58] “Defending the Digital Frontier.” *The Economist*, July 12, 2014.

[59] “Hackers Inc.” *The Economist*, July 12, 2014.

The UN approach to cybersecurity is based on four pillars: (1) protection of each organisation's own networks; (2) providing (coordinated) assistance to Member States[60] for the development of national cybersecurity-related policies and their implementation; (3) inclusion of cybersecurity in development programmes; and (4) fostering international cooperation on matters of cybersecurity, cybercrime, and the protection of human rights online – particularly privacy and access to information. This article mainly focuses on the last three pillars, since they are most relevant to the overall "Quest for Cyber Confidence," the theme of this publication. This section focuses on each one of them.

The UN considers that these three priorities for global cybersecurity share some common principles. Firstly, and in order to effectively secure information technologies, the UN vouches for a holistic, "whole-of-government" and multi-stakeholder approach. The internal work of the UN should follow this doctrine, and transition towards an "inter-agency" approach where relevant entities coordinate their work, thus becoming more efficient and avoiding duplication of effort. Secondly, given the dynamic nature of information technologies, the UN recommends flexible and frequently reviewed policies that are as technology-neutral as possible. Finally, the impact of security measures on other global priorities, such as the protection of individual privacy, should be prioritised in policy development.

Assistance to Member States

UN agencies have for long been involved in assisting Member States in matters of ICT development. Not until recently, however, has cybersecurity been considered a priority. With the development of a UN-wide Framework on Cybersecurity and Cybercrime, and its endorsement in 2013, the UN Chief Executives Board for Coordination[61] reached agreement on some common principles to follow when assisting Member States. The Framework is a first step towards harmonising internal UN efforts on matters of cybersecurity, and will be addressed at a later stage[62].

Inclusion of Cybersecurity in Development Programmes

ICT development (of which cybersecurity is a part) has generally been seen as a separate priority from other traditional areas of development. As a result, other areas

[60] Within each agency's mandate and respecting national sovereignty.

[61] See para 85 of the CEB Second Regular Session Report for 2013 (November 2013).

[62] See section on "UN Mechanisms for Cybersecurity."

have been considered more compelling and pressing than that of cybersecurity. However, ICT development is not at odds with the overall themes of sustainable development: rather than a goal in itself, technological development allows countries, particularly developing and Least Developed Countries (LDCs), to enhance their capabilities in a wide range of economic areas, improving also social welfare and overall living standards. Examples abound where technology has improved access to clean water, education and affordable health care, besides boosting economic growth and increasing/facilitating international trade.

It is thus imperative to include cybersecurity in *existing* development priorities: secure and trustworthy systems improve the likelihood of their adoption. In this regard, developing countries and LDCs have an exceptional window of opportunity: by aiming to develop inherently secure computer networks, they can leapfrog systems that are already experiencing attacks. Investment in cybersecurity can further help bridge the so-called "digital divide". The UN system can have an essential role in this by leveraging existing international mechanisms for mainstreaming cybersecurity programming.

An additional global priority is to prevent the emergence and escalation of cyber conflict. Although so far countries have shown restraint in responding to cyber attacks[63], this cannot be assumed to continue in the mid- and long-term. Through its research and educational efforts, the UN Institute for Disarmament Research (UNIDIR) seeks to contribute to the prevention of conflict escalation, as it "[…] serves as a bridge to create the necessary synergies to address and mitigate the effects of insecurity at the international, regional and local levels."

Fostering International Cooperation on Cybersecurity

Although online activities are subject to diverse regulation across jurisdictions, the Internet itself essentially remains a global network. This is especially true in matters of cybersecurity, where attacks and threats cross national borders on a daily basis. Such was the case, for example, with Conficker, the worm that managed to spread to over 180 countries[64]. No single country can address cybersecurity concerns, and the UN has set fostering international cooperation on matters of cybersecurity as a global priority.

[63] Valeriano, B., & Maness, R. C. (2014). "The dynamics of cyber conflict between rival antagonists, 2001-11." *Journal of Peace Research*. doi:10.1177/0022343313518940

[64] "Conficker." ShadowServer. Shadowserver Foundation, n.d. Web. 4 Nov. 2013.

A UN priority for ensuring trust in cyberspace is its consideration for the protection of human rights online. Particularly salient priorities are privacy and the right to information. The former is threatened by various actions including constant data breaches, and insufficient investment in data protection. The right to information is dependent on access to secure ICTs that allows freedom of expression and open access to public content. ICT security programmes must recognise these competing interests, as has been shown to be the case in the domestic policies of many, primarily developed, countries[65]. The R-O-A-M principles, which state that the Internet should be: Human **R**ights-based; **O**pen; **A**ccessible to all; and nurtured by **M**ulti-stakeholder participation, provide a solid basis for further work in this regard. The UN Educational, Scientific and Cultural Organization (UNESCO), the UN agency with significant expertise in the protection of human rights worldwide, has set this broader cybersecurity view as a priority for sustainable development.

Given the predominance of private actors in the Internet economy, and even In the management of the network itself, efforts to attain such protection should be made in coordination with stakeholders beside governments, including industry, the technical community, and civil society. This increased cooperation is especially critical with respect to legal investigations, where mutual assistance can be beneficial to all parties involved.

Basic Guidelines for Cybersecurity

Cyberspace's emergence as a comprehensive domain for international communications has brought – alongside the countless benefits of a more interconnected world – significant threats to the security and stability of UN Member States. Information confidentiality, computer systems, critical infrastructure and networked services are all vulnerable to Internet-based attacks that originate worldwide on a regular basis. Securing cyberspace in such circumstances[66] requires an approach that is:

- holistic (or "whole-of-government") since the prevention[67], detection, mitigation, and prosecution of cyber attacks involve a myriad of government and private entities;

[65] See *supra* at 2.

[66] This section is not a comprehensive census of UN guidelines for cybersecurity; rather, it is a basic summary of common trends found in the reviewed literature.

[67] Including building capabilities at the user level

- includes stakeholders involved with ICTs, including policymakers, Internet and telecommunication providers, technical organisations, and non-governmental organisations focused on protecting human rights (or “civil society”);
- encourages flexible and dynamic policies that can cope with the ever-changing spread of technologies, allowing room to respond to previously unknown (“zero-day”) threats and vulnerabilities, while keeping innovation unhampered; and
- respects human rights, particularly the right to privacy and access to information.

United Nations Mechanisms for Cybersecurity

Various salient UN cybersecurity frameworks with global impact are already in place, including the UN-wide Framework on Cybersecurity and Cybercrime; the World Summit on the Information Society’s (WSIS) Action Line C5: “Building confidence and security in the use of ICTs”; and the Information, Communication and Technology Network (ICT Network). Each will be described in the following subsections. This section also presents selected mechanisms for cybersecurity that are presently in the making in the UN system.

UN-wide Framework on Cybersecurity

As part of ongoing UN efforts to mitigate cyber threats, the UN-wide Framework on Cybersecurity and Cybercrime provides guidance to all UN entities in their quest to respond to Member States’ concerns regarding these issues and aims at strengthening coordination between them to increase confidence and security in cyberspace.

Criminal activities on the Internet vary greatly in their scope and frequency. The Framework attempts to address a significant portion of these threats by setting out basic principles to be followed by all UN entities, within their respective mandates. This UN-wide effort focuses on crime prevention and early warning, building domestic capabilities, effective deterrence, and promotion of justice against cybercrime activities. The Framework includes technical and capacity building aspects of assistance to Member States, using a holistic approach to enhance awareness and cyber-threat response capabilities.

As defined by the Framework[68], cybersecurity refers to the set of documents, practices, policies and technologies used to "[…] ensure the establishment and maintenance of the security properties" of relevant organisations, information, systems and assets. What does cybersecurity protect from? Besides providing increased trust in information technology, cybersecurity fences off computer-related criminal activity, or cybercrime[69]: a set of "[…] themes [that] include crimes against confidentiality, integrity and availability of computer data" and infrastructure; and a set of "… [criminal] computer-related acts" as well as data-related acts.

Principles related to Cybersecurity and Cybercrime

In order to ground the broad scope of the UN-wide Framework, the document is organised around seven broad principles that can more easily be translated into specific policies. These can be summarised as follows:

1. UN entities should help Member States in dealing with cyber incidents in a holistic manner, including through the delivery of technical support for criminal justice and strengthening of international cooperation.
2. The UN entities' own mandates should be considered when addressing Member States' needs, and cooperation should be sought with other relevant UN organisations.
3. All UN cybersecurity and cybercrime programmes should respect human rights and the rule of law.
4. UN programming should, where possible, assist Member States to adopt an evidence-based approach when conducting crime and risk assessments.
5. A "whole-of-government" response model that involves all key national stakeholders, as well as non-State actors, such as NGOs, academia and the technical community should be promoted where possible.
6. Support to Member States should aim to strengthen relevant formal and informal mechanisms for international cooperation on matters of cybersecurity and cybercrime.
7. Public-private cooperation within Member States, as well as the harmonization and adoption of technical policy and security standards and

[68] The Framework uses the International Telecommunication Union's definition, as outlined in "Recommendation ITU-T X.1205".

[69] As defined in the Framework.

guidelines on a regional and international level, should be encouraged, as necessary for an effective response to cyber threats.

Assistance to Member States is thus at the core of the Framework: it strives to improve cybersecurity and make the Internet a safer, more trustable space. Recommendations to implement the aforementioned principles, and effectively deliver such assistance, are outlined in the Framework. These guidelines can be classified as belonging to three categories: legal and policy measures, technical assistance, and mechanisms of implementation.

Technical Assistance

In an intrinsically technical domain such as cyberspace, capacity building and training in core cybersecurity skills within Member States is considered essential. The Framework recommends full in-country technical capability assessments as indispensable starting points and the elaboration of national cybersecurity policies. More specifically, technical assistance by UN entities could include: technical publications on cybercrime and its economics; information sharing mechanisms (best practices and other forms of generalisable knowledge); training in computer forensics and other cybercrime investigation skills, including end-user education in secure computer and network usage; cooperation with private Internet Service Providers (ISPs) and other relevant stakeholders in data collection and analysis; computer incident response, including the creation of permanent institutions to deal with incidents (such as national Computer Incident Response Teams – CIRTs) and "central contact points for requests from abroad".

WSIS Action Line C5

As outlined in the WSIS Summit (2003)[70] outcome documents and reviewed during the WSIS+10 High-Level Event (2014), WSIS Action Line C5 focuses on building confidence and security in the use of ICTs and its facilitation responsibility was assigned to the ITU. In 2007, the ITU launched the Global Cybersecurity Agenda (GCA) "[…] to provide a framework within which the international response to the growing challenges to cybersecurity can be coordinated and addressed" with Member States and other relevant stakeholders. In this regard the ITU has developed partnerships with all stakeholders around the world for cybersecurity development towards, *inter*

[70] World Summit on the Information society http://www.itu.int/wsis/index.html last updated 13.10.2014

alia, publishing guidelines for national policymaking on cybersecurity[71], providing technical assistance to Member States to develop national capabilities, and fostering inclusive discussions on the necessary technical standards to enhance security.

ICT Network

A mechanism of the UN Chief Executives Board for Coordination, the ICT Network pools ICT capabilities in policymaking from many UN entities. It coordinates and serves as a forum to develop and implement policies related to ICTs. Most relevant for this publication, however, is its Information Security Special Interest Group, which explores issues related to cybersecurity "[…] through both expert and case-study presentations, [and examination of] inter-agency areas of action, including incident response, information security and policies, and information security awareness"[72].

Ongoing efforts

As both UN Member States and the CEB have recognised[73], there is a need for a concerted effort in the UN system in matters of cybersecurity and cybercrime. Following endorsement of the UN-wide Framework on Cybersecurity and Cybercrime in 2013, UN Secretary-General Ban Ki-Moon called for ITU, – together with UNESCO, UNODC, UNDP and UNCTAD, and in close coordination with the High-level Committee on Management (HLCM), the High-level Committee on Programmes (HLCP), and the UN Development Group (UNDG) – to develop a system-wide comprehensive and coherent strategy for addressing the relevant issues, for discussion at the second regular session of the CEB in November 2014[74] – an ongoing effort.

Conclusion

There is global consensus on the need for a comprehensive, global response to the issues of cybersecurity. The UN is addressing these issues following a holistic, multi-stakeholder, human rights-respectful, flexible and dynamic model. Although there still is no agreement on a vision for cybersecurity, some common elements and trends

[71] ITU National Cybersecurity Strategy Guide, September 2011.

[72] Information Security Special Interest Group. UN - Chief Executives Board for Coordination, 2014. Web. 22 July 2014.

[73] "Action on Cybersecurity/Cybercrime and Policies on Information." UN - CEB, 21 Nov. 2011. Web. 22 July 2014.

[74] See para 85 of the CEB Second Regular Session Report, November 2013.

exist in the work of UN entities that highlight the recent prevalence of cybersecurity as a global priority. It is now recognised that securing cyberspace is a universal need with clear impacts on economic and social development, while it is also critical to balance competing interests and respect national sovereignty. The future prospects for cybersecurity seem bright, as recognised by Choucri et al[75] : "Although the current system of [international] institutional arrangements [on cybersecurity] shows signs of weakness, it is also true that the level of organisation and cooperation has been steadily increasing."

This positive trend is an additional incentive for international cooperation in cybersecurity; given the global nature of the Internet, only efforts with worldwide (or quasi-worldwide) reach can be effective in securing cyberspace. The costs of service disruption following cyber attacks can be quite high, especially in critical sectors such as power distribution or finance, but the benefits of investing in cybersecurity far outweigh them. This calculation is accentuated for developed countries with highly interconnected infrastructure. Developing countries, on the other hand, are seeing a historic opportunity to leapfrog their development, and prioritising cybersecurity can certainly boost those prospects.

These changes will only become a reality when cybersecurity is made a truly global priority. The UN, with its significant expertise in development in emerging domains, is best positioned to become a global facilitator for international cybersecurity efforts; States, industry and civil society can all greatly benefit from contributing to them.

Chapter II: Cyber Resilience

Introduction

In February 2005, the US President´s Information Technology Advisory Committee issued a call to action[76] to strengthen security in cyberspace[77] in a landmark report entitled "Cyber Security: A Crisis of Prioritization". A related topic featured in a list of

[75] See *Supra* at 2.

[76] President's Information Technology Advisory Committee, "Cyber Security: A Crisis of Prioritization" (February 2005)

[77] National Academy of Engineering: "Grand Challenges for Engineering"; http://www.engineeringchallenges.org/cms/challenges.aspx

the "14 Grand Challenges for the 21st century" was published by the US National Academy of Engineering in 2008. In recent years, many other sources have also addressed this challenge for cyber confidence in the future digital world.

Since then, mankind's dependency on the benefits of the digital age has continued to grow exponentially as computing and communication devices and systems become ever more ubiquitous and essential to virtually every aspect of our everyday lives.

Hence the crucial importance of keeping cyberspace safe and of building resilience to withstand the growing threat of cyber attacks that have the potential to wreak havoc and destruction on a massive scale.

Ever increasing usage of sensor technologies, cyber-physical systems, cloud services, big data or self-adaptive, intelligent systems[78] will greatly expand the capabilities of ICTs and influence everyday life as we move inexorably towards the Internet of Things.

This trend is not only driven by technological advances but also by relentless new market and product demands. Expanding cyber infrastructure and services will offer increased opportunities and benefits, but also give rise to additional vulnerabilities and new threats capable of undermining the private and public safety and security of our societies.

The stakes are high, not least because confidence in the digital age and even our overall well-being largely depend on our ability to identify and manage a wide range of cyber threats. Based on careful vulnerability and risk analyses and assessment, adequate measures have to be developed to assure cybersecurity – or at least adequate cyber resilience – especially in relation to critical infrastructure such as energy, water, transport, health and financial systems[79].

Sources of potential risk to cyber stability and security include the increasing complexity and use of ICT infrastructures and services. Even more critical are threats posed by external events such as environmental disasters or attacks by governments, criminal organisations or individuals. Research has shown that even system designers, operators and users can be a major source of ICT vulnerability – intentionally or

[78] Markus Luckey Gregor Engels: "High-Quality Specification of Self-Adaptive Software Systems". In: Proceedings of the 8th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. ACM (New York, NY, USA), SEAMS '13, pp. 143-152; (2013)

[79] US Executive Order 13636: "Improving Critical Infrastructure Cybersecurity"; (February 2013): http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

unintentionally. In this regard, the basic scientific and technical problems that must be addressed relate to “complexity-emergency-resilience” issues in cyberspace.

First, this chapter clarifies terminology with respect to ICT complexity, resulting cyber risks and unexpected system behaviour, and the growing need for adequate cyber resilience strategies. It then outlines the numerous potential sources of cyber risks – ranging from physical, technical or environmental errors and failures to organisational, institutional or legislative causes – and discusses cyber risk identification, analysis and resilience strategies up to the information level from a computer science and engineering point of view. The following chapters are heightening resilience challenges for “big data”, “cloud computing” applications, as well as for demands of resilient cyber control systems. Finally, this chapter includes contributions on cyber resilience from the private sector perspective, considers a major non-technical cyber risk and proposes an urgently required international legal framework to counter existing risks beyond the data protection dimension.

Chapter 2.4 considers a major non-technical cyber risk and proposes an urgently required international legal framework to counter existing risks beyond the data protection dimension.

2.1 Foundations of Cyber Resilience

By Axel Lehmann

Terminology

As already stated, a real challenge in the development of CBMs is the increasing complexity of the digital world that influences everyday public and private life. In general, the **complexity of a (digital) system** depends on the number and functionalities of its components which determine a system´s state space.

Super computers are at the top end of performance levels and their peak performance is expected to be in the order of 1000 PetaFLOPS – 100 quadrillion floating point operations per second – within the next decade[80]. Cyber-physical systems (mostly invisible, embedded micro computing devices offer only very specialised and limited computing capabilities.

[80] Exascale Computing: see: http://en.wikipedia.org/wiki/Exascale_computing

Enlarged interconnectivity between the diverse systems enables the formation of so-called "system-of-systems" (used for example to regulate energy, communications or traffic control systems)[81]. Information storage is another important global service that has to be taken into account regarding cyber confidence; storage technologies are evolving even faster than computer technologies (permanently increasing storage capacities at significantly decreasing cost).

With the increasing number both of the components and capabilities in a system and in the number of systems interconnected within scalable "system-of-systems", the overall system complexity that has to be mastered is growing exponentially.

These ongoing technological advancements require especially robust design, development and quality assurance methods to guarantee system stability, availability – as well as resilience strategies in case of undesired situations[82] – and cyber confidence. Increased application of formal methods for system specification and design can ensure that certain (unsafe or critical) system states can be detected and avoided if adequate identification and prevention measures are implemented. However, events or hazards that could not be foreseen during design may lead to unexpected or emergent system behaviour that might be difficult or even impossible to control or adjust. In a worst-case scenario, the system could collapse and not be repairable to an operational state. For all these reasons, adequate cyber resilience methods must be developed and implemented.

Such threats, vulnerabilities and risks have to be identified, analysed, evaluated and counter-measures developed. Designing digital systems with formally proven design and fault-tolerance methods will significantly improve their robustness and controllability, but will not completely avoid emergent behaviour especially within a system-of-systems configuration. Therefore, adjustment methods and procedures must be explored and implemented to improve **the resilience of systems and processes** as an important step toward establishing confidence in them and in cyber space generally.

[81] Mo Jamshidi: "System-of-systems engineering: a definition"; In: IEEE SMC; (2005).

[82] "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; Published by Ashgate Publishing Limited; (2006).

According to Wreathall´s definition[83], "[…] resilience is the ability of an organisation (system) to keep, or recover quickly to, a stable state, allowing it to continue operations during and after a major mishap or in the presence of continuous significant stresses**."** At the 2012 World Economic Forum the initiative "Partnering for Cyber Resilience" was established, and some "Principles and Guidelines regarding Risk and Responsibilities in a Hyperconnected World" were formulated[84]. Given the huge variety of human users, designers, operators, digital devices and systems that make up this complex digital world, and as research has shown that the most vulnerable entities therein are humans, their activities have to be especially considered in the context of confidence-building measures.

Identification and classification of Cyber Risks

In a world where humans are so reliant on cyber resources, cyberspace risk and resilience analyses have to consider a wide range of perspectives covering both human actors as well as the variety and complexity of the digital age. The spectrum of cyberspace resources ranges from global digital infrastructures and services that can be used worldwide to stand-alone computing or cyber-physical devices.

Also, with respect to human activity in cyberspace – e.g., as designers, developers or users – we have to distinguish their roles and capabilities in using digital systems either as insiders or outsiders. In hierarchical terms, as well as for classification of cyber risk identification, analysis and preventive, the following abstraction levels or layers can be distinguished. As disruptions and deficiencies evolving at lower levels can significantly influence system behaviour and operation at higher levels, an overall risk analysis and risk assessment has to consider all the following factors as a prerequisite for the development of system resilience strategies[85],[86]:

- Global level

[83] John Wreathall: "Properties of Resilient Organizations: An Intitial View"; In: Resilience Engineering – Concepts and Precepts, Ashgate Publishing Limited; (2006).

[84] World Economic Forum: "Partnering for Cyber Resilience"; February 2013 Newsletter – Davor Special Edition;http://www3.weforum.org/docs/WEF_RRHW_PartneringCyberResilience_NewsletteFebruary_2013.pdf; (2013)

[85] "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; Published by Ashgate Publishing Limited; (2006)

[86] Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; In: K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg; (2012)

- Enterprise layer/institutional/private level
- Information level
- Technical level
- Physical level

Cyber Risk Analysis & Cyber resilience from a Computer Science or Engineering Perspective

In order to develop sound cyber risk analysis and cyber resilience strategies, major sources of cyber risks must first be identified at each of the aforementioned levels. As a second step, any side effects (dependencies) must be carefully analysed and evaluated, as an error, fault, failure or intrusion at a lower level may influence functionalities, reliability or confidentiality and security at higher levels. For this purpose, dependency graphs[87] are used to detect mutual dependencies by forward- and back-tracking the level paths towards each other, which allows for detection of causes of malfunctions, faults, failures, leaks or corrupted data.

As illustrated in Figure 1 below, each level provides certain capabilities, functionalities or services (cx) that incorporate or use lower level attributes. as indicated by directed arcs. The dotted arcs indicate that implementation of each capability (cx) requires compliance with certain standards, regulations or rules. In Figure 1, a deficiency is identified at the enterprise level, possibly caused by an error, fault or an intrusion in that node or in a lower level node. By traversation of the graph structure (backward and forward chaining in the graph structure) potential sources of an error, fault or failure can be located.

[87] Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: “Basic Concepts and Taxonomy of Dependable and Secure Computing”; IEEE Transactions on Dependable and Secure Computing; (2004)

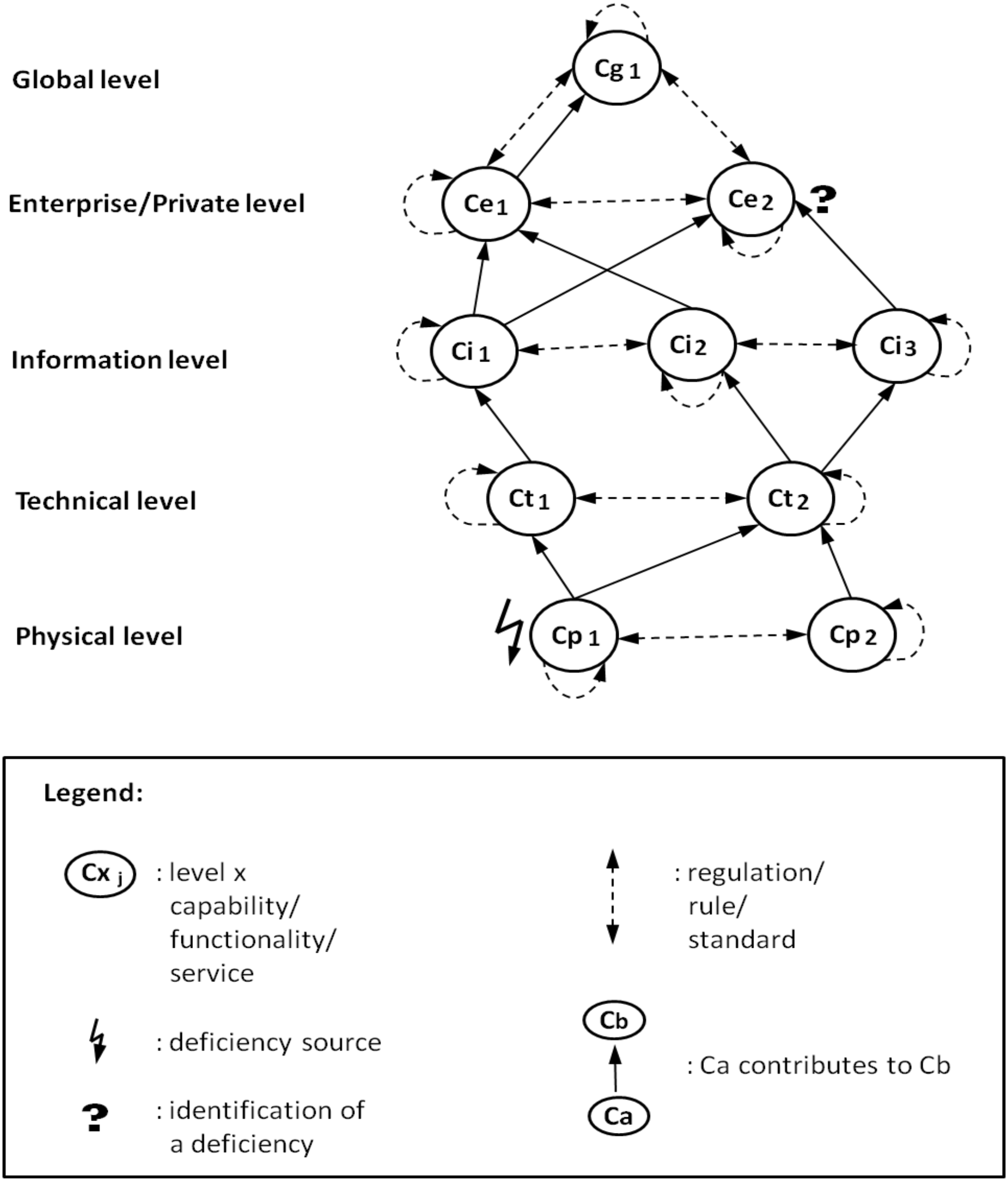

Figure 1: Example of a dependability graph

As already mentioned, the rapid evolution of ICTs enable significant technical advancements but at the same time brings new sources and causes of cyber risks that impact cyberspace stability and security. Besides physical and technical deficiencies, major cyber risk sources stem from the trend towards virtualisation of computing, communication and storage resources driven by demand for increased performance, reliability, and cost-effectiveness for the user community. This trend is evidenced by rapidly evolving technologies such as big data, cloud computing and cloud -based software as a service (SaaS) facilities[88] , system-of-systems[89], and "hyper-networks"[90].

These technological developments also see the emergence of new cybersecurity issues in relation to privacy, confidentiality and authenticity. Apart from the misuse, manipulation and corruption of data and ICT infrastructures, these technologies trigger new risks for the unauthorized collection, usage and merging of personal or other confidential data. The danger – already a reality in some cases - is that multiple types of proprietary data of individuals, organizations or even States are becoming "glassy", undermining confidence in cyberspace.

In general, risks can be calculated according to:

$$\text{Risk} := \text{Likelihood} * \text{Impact}$$

From a technical standpoint, cyber risks can be caused by design errors, faults, failure of digital components during operation, malfunctions or by emergent system behaviour especially in "hyper-networked" system configurations. In addition to the risks can arise from erroneous usage or malpractice of digital systems, as well as by attacks of insiders, users, and even by unexpected accidents or environmental events. To minimize those ICT-related risks, a more precise relation for risk analysis has to be considered: ICT-Risk := f (Threat, Vulnerability, Asset).

In the context of ICT, the vulnerability of an ICT system relates to weaknesses or deficiencies in its design, implementation, or erroneous applications, which can cause faults, reduced capabilities, system component malfunction, or even system collapse. Such vulnerabilities must first be identified and classified before considering possible remedial options. In this regard, ICT-related risk assessment has to be performed

[88] Nicolas Gold, Andrew Mohan; Clair Knight, Malcolm Munro: "Understanding Software-Oriented Software"; In: IEEE Software; (2004)

[89] Mo Jamshidi: "System-of-systems engineering: a definition"; In: IEEE SMC; (2005)

[90] "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; Published by Ashgate Publishing Limited; (2006)

followed by prioritisation of ICT infrastructure and service vulnerabilities and corresponding countermeasures. Quantitative risk analysis could then be performed for example by:

ICT-Risk := ((Vulnerability * Threat / Score of Counter measure) * Asset Value.

Prerequisites for development of an ICT resilience strategy are reliability (or dependability) and availability analyses which should consider the following generic methods to improve system reliability and availability[91]:

- *Fault prevention* – to avoid the occurrence of errors and faults by careful design and implementation;
- *Fault removal* – to detect the existence of errors that might result in a fault or even failure by application of test, verification and validation methods;
- *Fault tolerance* – to provide redundancy (e.g. by duplication of resources and/or by diversification of implementations) which can cover and adjust faults if these occur;
- *Fault/Failure forecasting* – to analyse and evaluate the consequences of faults which can cause a system to fail and the consequences of system operation[92].

From an analytic point of view, dependency graphs (like in Figure 1) or reliability block diagrams are simple methods to analyse effects and side effects of errors, faults, failures as well as of specific countermeasures as mentioned above[93] .

Apart from these ICT-related vulnerabilities, other threats caused by deficiencies have to be considered with respect to cyber confidence. "A threat is a potential danger that might exploit a vulnerability to breach security and thus cause harm. Therefore, additional threats that result from human user activities on system resources, from accidents, natural disasters or from other unexpected external events have to be considered and assessed."[94]

[91] Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: "Basic Concepts and Taxonomy of Dependable and Secure Computing"; IEEE Transactions on Dependable and Secure Computing; (2004)

[92] Ibid

[93] Ibid

[94] Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; In: K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg; (2012)

Human activities causing threats can be performed either intentionally (e.g., by insiders, hackers), or unintentionally through user operation or behaviour. For risk analyses, the most probable human activities causing harm should be identified and resulting vulnerabilities analysed. Besides vulnerabilities and threats, cyber risk analyses have to consider their influence on a system´s capabilities, assets and the respective asset values.

The following approaches should be considered in developing cyber resilience[95]:

- Deficiency prevention – to avoid the occurrence of deficiencies such as errors, faults and failures at physical and technical levels by careful design, implementation and operation of a system and of operation procedures; at the higher levels this can be achieved by following accepted level-specific standards, regulations or rules of behaviour;
- Deficiency removal – to detect the existence of deficiencies that might result in a fault, failure, malfunction or misuse by application of test, verification and validation methods;
- Deficiency tolerance – to provide redundancy, e.g., by duplication of resources and services as well as by diversification of implementations which can cover and adjust deficiencies if these occur;
- Deficiency forecasting – to explore vulnerabilities in plausible scenarios through massive simulations, analysis of corresponding risks, and evaluation of the consequences of resilience strategy implementation within that context.

To develop an overall resilience strategy based on those risk and reliability analyses requires in addition adjustment and recovery mechanisms which enable a system to fully recover on its own from an unavailable state, from degraded performance states or from intrusion. Most natural or biological systems have developed mechanisms for self-healing or self-reconfiguration. For technical systems, such bio-analogue processes or organisations – called organic computing capabilities – respective coverage, adjustment and recovery methods have to be explored and presumed at system design stage. Scientific research on organic computing and communication is focusing on such bio-analogue methods that can improve the resilience of ICT and cyber-physical systems – concepts for implementation of self-x digital systems (x

[95] Ibid

replaced by e.g. protecting, healing, optimizing, configuring[96]. Based on research results in areas like knowledge engineering or data mining, design principles of intelligent systems have evolved and can be applied for permanent risk identification and evaluation, as well as for taking predictive actions to enable system resilience.

Starting bottom up, level-specific measures to avoid or recover from faults, malfunctions, failures or disruptions and for improving cyber resilience from a computer engineering perspective are for example[97],[98],[99]:

- on the physical level - restrictions regarding the use of materials and devices only under predefined environmental conditions (e.g. regarding temperatures, radiation). In addition, redundancy can be implemented by use of alternative materials, optional operational processes etc. as well as by diversification of a components implementation ;
- on the technical level - (n out of m) computing devices, redundant data transmission and data coding concepts or usage of different but standardized secure transmission protocols offer opportunities not only to avoid fault propagations but also enable self-adjustments. Also diversification, such as diverse implementation of computing algorithms, diverse computing nodes, or use of different storage concepts are measures to avoid fault propagation, to increase system reliability and to enable resilience on the technical level[100];
- on the information level – goal is "Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." -

[96] “Organic Computing”; Ed. Rolf Würtz; In: Springer series Understanding Complex Systems; Springer (2008)

[97] Yue Yu, Michael fry, Alberto Schaeffer-Filho et.al.: “An Adaptive Approach to Network Resilience: Evolving Challenge Detection and Mitigation”; In: 8th IEEE Internat. Workshop on the Design of Reliable Communication Networks; (2011)

[98] Dorothy Reed, Kailash Kapur, Richard Christie: “Metzhodology for Assessing the Resilience of Networked Infrastructure”; In: IEEE Systems Journal, Vol. 3 No. 2; (2009)

[99] Piotr Cholda, Anders Mykkeltveit et. al.: “A Survey of Resilience Differentiation Frameworks in Communication Networks”; In: IEEE Communications, Surveys, Vol.9 No.4; (2007)

[100] USA Department of Energy: “21 Steps to Improve Security of SCADA Networks”; (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

(ISO/IEC 27000[101]. Measures are for example redundant coding or use of robust encryption / decryption algorithms, or secure data transmission protocols to prevent faults, misuse or corruption; regarding tools, SCADA (Supervisory Control and Data Acquisition) systems and networks can be installed[102] on the enterprise / private level, to follow established best practices, business, workflow and security standards, rules and restrictions as well as internal codes of conduct[103];

- on the Enterprise/institutional/private level– a framework of laws and rules of operation; institutional, regional and cultural codes of conduct; adequate education; dissemination of information and training to improve cybersecurity awareness;
- on the global level – to follow worldwide accepted political agreements and – as far as available - global codes of conduct; more specifically, to establish a framework of international laws and rules of operation, to introduce and respect regional and cultural codes of conduct; to establish adequate education; to disseminate of information materials and to offer training opportunities to improve cybersecurity awareness.

This is by far a non-exhaustive list of measures and methods to improve cyber security and – also as a consequence – cyber confidence.

2.2 Heightening the Resilience of Cloud Computing and Big Data Systems

By Vladimir Britkov

The main new ICT developments are big data and cloud computing. Gartner estimates that 64% of organisations worldwide have or plan to invest in big data. The latter are

[101] ISO/IEC27000-Standard: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary; (2014)

[102] USA Department of Energy: “21 Steps to Improve Security of SCADA Networks”; (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

[103] Amy Lee, John Vargo, Erica Seville: “Developing a Tool to Measure and Compare Organizations Resilience”; In: Nattural Hazards Review; ASCE, February (2013)

massive amounts of digital information about human beings and our environment that are expected to double every two years. Big data technology includes the new field of "Business Intelligence" the analytics, which allows for greater cyber resilience in the fields of big data and cloud computing.

Large-scale cloud infrastructures, the volume and diversity of data sources and formats, the streaming nature of data acquisition, and high- volume inter-cloud migration all create unique security vulnerabilities. Therefore, traditional security mechanisms, which are tailored to securing small-scale, static (as opposed to streaming) data, are inadequate. In this paper, we highlight the top ten big data security and privacy challenges which it is hoped will lead to increased focus on fortifying big data infrastructures.

Trust – a "must" factor between a cloud-based service provider and a client for fruitful business – is one of the most prominent security issues. However, there is no particular trust bond to ensure that no insider attack or other security incident will target information on the cloud. Companies naturally consider this a major factor when engaging in business activities with a cloud-based provider. Clients can, however, establish a Service Legal Agreement (SLA) with the cloud provider which stipulates the terms and conditions of the contractual relationship between a client and a cloud service provider. SLAs have particular relevance in regard to the protection of client data hosted in the cloud service but, given the global nature of the cloud, it usually spans many jurisdictions, with often varying applicable legal requirements.

Big data infrastructures were formally typically proprietary and isolated from general networks. Combined with the adoption of data mining methodologies, big data is now cheaply and easily accessible to organisations large and small through public cloud infrastructure. Software infrastructures enable developers to easily leverage thousands of computing nodes to perform data-parallel computing. In order to protect the infrastructure of big data systems, the distributed computations and data stores must be secured. To secure the data itself, information dissemination must be privacy-preserving, and sensitive data must be protected through the use of cryptography and granular access control.

Managing the enormous volume of data necessitates scalable and distributed solutions for both securing data stores and enabling efficient audits and data provenance. Finally, the streaming data emerging from diverse end-points must be checked for integrity and can be used to perform real-time analytics for security incidents to ensure the integrity of the infrastructure.

The top ten challenges to big data security and privacy:

1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transactions logs
4. End-point input validation/filtering
5. Real-time security monitoring
6. Scalable and composable privacy-preserving data mining and analytics
7. Cryptographically enforced data-centric security
8. Granular access control
9. Granular audits
10. Data provenance

Towards secure big data infrastructure

Solving security and privacy challenges typically requires addressing three distinct issues:

1. Modelling: formalizing a threat model that covers most cyber-attack or data-leakage scenarios.
2. Analysis: finding tractable solutions based on the threat model.
3. Implementation: implementing the solution in existing infrastructures.

Towards Secure Computations in Distributed Programming Frameworks

Use Case: Modelling

The threat model for mappers has three major scenarios:

1. Malfunctioning Compute Worker Nodes – Workers assigned to mappers in a distributed computation could malfunction due to incorrect configuration or a faulty node.
2. Infrastructure Attacks – Compromised Worker nodes may tap the communication among other Workers and the Master with the objective of replay, Man-In-the-Middle, and DoS attacks to the MapReduce computations.
3. Rogue Data Nodes – Rogue data nodes can be added to a cluster, and subsequently receive replicated data or deliver altered MapReduce code.

Analysis

Based on the threat model outlined above, there are two dimensions of analysis: ensuring the trustworthiness of mappers and securing the data despite untrusted mappers. For ensuring the trustworthiness of mappers, there are two techniques: trust establishment and Mandatory Access Control (MAC).

Implementation

MAC is implemented by modifying the MapReduce framework, the distributed file system, and the Java virtual machine with SELinux as the underlying operating system.

Conclusion

Big data is here to stay. It is practically impossible to imagine the next application without it consuming data, producing new forms of data, and containing data-driven algorithms.

As computing environments become cheaper, application environments become networked, and system and analytics environments become shared over the cloud, security, access control, compression, encryption, and compliance introduce risk challenges that must be addressed in a systematic way. These challenges are reflected in the top ten security and privacy problems highlighted above that need to be addressed to make big data processing and computing infrastructure more secure and resilient.

Common elements specific to big data arise from the use of multiple infrastructure tiers (both storage and computing) for processing it; the use of new compute infrastructures such as NoSQL databases (for fast throughput necessitated by big data volumes) that have not been thoroughly vetted for security issues; the non-scalability of encryption for large data sets; the non-scalability of real-time monitoring techniques that might be practical for smaller volumes of data; the heterogeneity of devices that produce the data; and the confusion surrounding the diverse legal and policy restrictions that lead to ad-hoc approaches for ensuring security and privacy.

2.3 Towards Resilient Cyber Control Systems

By Stefan Lüders

Life in today's "Westernised" world is determined by control systems which regulate virtually all aspects of our daily lives. Our lives are in symbiosis[104] with control systems and are inextricably dependent on them. Without them, our existence would rapidly devolve to resemble living standards in the Middle Ages[105]. Given our dependency on these control systems, ensuring their stability and resilience is essential.

Today, however, these control systems have become vulnerable to the deficiencies of the standard IT systems that operate them. They use the same techniques found in modern computer centres: the Ethernet protocol, TCP/IP, the World Wide Web and electronic mail have replaced proprietary fieldbus communication; PCs eliminate the need for manual displays, gauges and panels; the Microsoft Windows operating system supersedes custom command line terminals.

Moreover, high quality software is rare and contains defects, flaws, errors and bugs. To meet market demand, software is shipped in beta state, eventually functioning but with inherent weaknesses and vulnerabilities that are detected (and fixed) later. Users and utilities do not necessarily request improvements because of the costs that would entail.

To make matters worse, standard IT has opened up a whole new market for criminal activity – a "dark net" where individual attackers team up to infiltrate and exploit IT systems, compromising user confidence. Today, every single Internet, website, operating system, and popular software application is constantly probed for vulnerabilities and weaknesses by ill-intentioned actors seeking to profit from them for their own benefit, or to sell them on the dark market. And since the overall task of preventing or fortifying resilience to these attacks is infinitely more complex than the exploitation of these vulnerabilities, the attackers benefit from a certain advantage.

[104] See also Stefan Lüders "Our Life in Symbiosis" CERN Publications, 2014.

[105] This is well depicted in the novel of Marc Elsberg "Blackout : Morgen ist es zu spät" Blanvalet, March 2012.

Still, overall IT has so far proven to be resilient enough to avoid large-scale impacts of these attacks on our daily lives, and even though the "dark" economy continues to flourish and the international legal system struggles to keep pace, the general public is rarely severely affected[106].

With the exponential development of control systems and their incorporation of standard IT, the game has changed. While these systems benefit from IT functionality, they have also inherited its vulnerabilities and weaknesses. This has made robust, proprietary and custom controls processes fragile and exposed – and increasingly tested by ill-intentioned actors, as illustrated in the following media headlines: "Russia welcomes hack attacks" (The Register, 2000), "Hackers hit Pennsylvania water system" (InTech, 2006), "TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds" (The Washington Post, 2008), "Insider charged with hacking California canal system" (Computerworld, 2009), "US air traffic exposed to 'serious harm' from cyber attacks" (Flightglobal, 2009), "Electricity Grid in U.S. Penetrated By Spies" (The Wall Street Journal, 2009), "Report: Hackers broke into FAA air traffic control systems" (CNET, 2009), "Report: Cyber Attacks Caused Power Outages in Brazil" (Wired, 2009), "DHS: America's water and power utilities under daily cyber attack" (Computerworld, 2012), "Sluices, pumping stations & bridges poorly protected" (Radio Netherlands Worldwide, 2012), "US Power Grid Vulnerable to Just About Everything" (OilPrice.com, 2012). Another recent highlight was the sabotage of the Natanz nuclear enrichment facility in Iran, reportedly by Israeli and US secret services: "Stuxnet Virus Opens New Era of Cyber War" (Spiegel Online, 2010). "Stuxnet"-infected Windows-based PCs, faked the displays shown to facility operators, downloaded itself into the controls processor, and subsequently manipulated the rotational speed of hundreds of centrifuges such that uranium enrichment became ineffective.

While "Stuxnet" is perceived as the very first documented cyber-sabotage event, it also reflects the dilemma of State-sponsored cyber attacks. Richard A. Clarke, a former White House National Coordinator for Security and Counterterrorism**,** has said that the US might be able to blow up a nuclear plant or a terrorist training centre somewhere, but that a number of countries could strike back with a cyber attack and that "the entire US economic system could be crashed in retaliation [...] because we can't defend it today".

[106] With the possible exception of attacks on the world wide domain name servers, on the Internet's core routes, and, more generally, on the privacy of citizens by some government bodies.

Indeed, it is currently not possible to protect control systems with similar techniques to those used to protect a facility such as a computer centre, for example by "patching" – i.e. fixing vulnerabilities by updating the operating system.

Modern computer centres are driven by configuration management systems. Updating or even the reinstallation of large batches of servers is usually possible within short time spans. Redundancies and virtualisation ease this process as sub-clusters of server farms are taken into maintenance while the core continues to serve operations. Flexible patching of control systems, on the other hand, is currently inhibited by rare maintenance windows and strict compliance requirements, in particular for relevant safety processes. Only fully compliant and certified systems (e.g., re-certification to a Safety Integrated Level, SIL) are considered safe. Thorough testing, however, takes time and comes with additional costs. Furthermore, it is not always guaranteed that new operating system patches are compatible with existing control system software, and vendors are usually late declaring such compliance, if they do at all. Embedded systems, which are hard to upgrade, add to this. Finally, while computer centre hardware is often recycled every three to five years, old hardware is kept in the controls process as long as possible, even well after the declared end of its operating system lifetime[107].

Another example is given through different approaches of access control. Computer centre services usually give priority to confidentiality, integrity and availability (i.e., "CIA"). Access control is, therefore, paramount and authentication and authorisation techniques are well embedded and centralised using single sign-on with or without multifactor deployments, x509 certificate management and centrally managed LDAP/AD directories. Control systems prioritise availability over confidentiality and integrity ("CIA"). Thus, human access to the process must always be guaranteed.

In order to facilitate the handover of operations, passwords are shared between operators. In addition, often due to their proprietary or legacy nature, hardware and software come with undocumented backdoors, run with unchanged default passwords, do not allow the blocking of unauthorised connections using internal firewalls or access control lists, and are hard to integrate into central identity management solutions. Encryption is considered too resource demanding. More likely, control systems require or rely on additional protective devices to keep them secured and access controlled. Proper network protection becomes even more important, but

[107] The recent phase-out of the Microsoft Windows XP operating system poses hence another challenge to utilities.

falls short as a good “defence-in-depth” paradigm requires protective means on every layer of the actual hardware of its operating system and applications.

Finally, robustness is of key importance. As mentioned earlier, standard IT systems in a computer centre, in particular when directly accessible from the Internet, are constantly probed for weaknesses by attackers. Such penetration and vulnerability scans can be countered if the centre is well managed, kept up-to-date in every aspect of this phenomenon and proper intrusion detection systems are in place and monitored. Decades of experience and knowledge of different attack scenarios and potential weaknesses, and accepted means of sharing information among stakeholders, make incident protection, detection and response easier. Conversely, control systems cannot be considered cyber-robust. While their physical hardware might be, their software implementation has repeatedly been shown to violate common IT standards, fail basic security tests, and lack fundamental means to repel them[108]. Control systems fulfil well-defined use cases, but fail when such cases are less well defined. Unlike standard IT hardware, “security” is not an integral part of control system devices. Even if they were, given that security implementation is proprietary and kept obscure, utilities face difficulties in asserting whether the security is really appropriate or just an illusion.

Last but not least, the control system community currently struggles to find consensus on how to conduct “responsible disclosure”, i.e. how to announce and publish newly found vulnerabilities to the corresponding vendor and, later, to the utilities community. In the standard IT world, a time frame of three to nine months between notification of the software provider and full disclosure to the public is accepted, but this is deemed by some to be too short a period given that software development life cycles for software controls are much longer, and that applying patches within the utility must be well coordinated and scheduled. In reality, this whole process normally takes about a year.

This issue must be overcome is control systems are to become cyber-resilient. Control systems must ensure that security becomes an integral part of overall functionality, availability, usability, maintainability and safety. Control system experts must engage in appropriate IT training and, in particular, IT security. Training must start at the educational level in colleges and universities with security integrated into curriculum, rather than considered as an “add-on”. Better still, all IT-related aspects should be

[108] “CERN tests reveal security flaws within industrial networked devices“, *The Industrial Ethernet Book*, 2006.

outsourced to competent IT specialists able to differentiate between the respective needs for running control systems and computer centres. New compromises might be necessary to rebalance the need for permanent availability and prompt patching, for easy access and tight access control. In parallel, IT virtualisation techniques might provide the panacea to overcome such problems and serve as a new basis for patch rollout staged between test, pre-production, and operational systems. Full software management, version control systems, 360° software development life cycles, thorough regression testing, and nightly builds must become standard for control systems, too. Integration into thoroughly populated and permanently up-to-date inventories is another “must”. A fastidious documentation of the installation base, of all devices, accounts, applications, including their inter-dependencies, is mandatory to understand risks and to deploy protective measures. Penetration testing must become a default. Ideally, widely agreed and fully open recipes and procedures to conduct vulnerability assessments become standard such that vendors and manufacturers, utilities and integrators, but also governments, academia and certification authorities can independently assess the security of given controls devices, hardware or software. Such procedures will imperatively increase the robustness of today’s control systems, eventually, improve their resilience to ill-intentioned activities, and hopefully pave the way towards a certification scheme à la ISO9001.

All these steps are neither trivial nor convenient. For the current generation of control systems and control system experts, it might even be too late. Therefore, we should focus on the future and aim at merging even more control system and computer centre IT. The level of our success will be the litmus test for determining the shape of our future.

2.4 Cyber Resilience from the Private Sector Perspective

By Danil Kerimi

Today we live in an enormously complex and hyper-connected world. It brings us unprecedented opportunities and risks unimaginable only a few years ago. We are only now starting to understand social, political and economic changes that it is generating by adjusting norms, policies and business models to the metaphysics of the network.

All these changes fundamentally redefine the way individuals, enterprises and governments interconnect with each other. The traditional methods of economic value creation and consumption are being challenged by new business models and social interactions caused by hyper-connectivity. Already now, industries increasingly rely on digital channels for their internal operations, as well as interactions with their partners. Entities that have never been thought of as core technology players now have to deal with issues that lie outside of their areas of expertise or comfort.

Consumer behaviour has shifted towards more empowerment, better information flows and abundance of choices. Companies now have more insight into consumer behaviour than ever before allowing for an unprecedented level of customization. They are also challenged to adapt to the fast moving landscape to ensure that new consumer expectations such as product co-creation and rapid prototyping are met.

Hyper-connectivity is becoming a catalyst that often reduces entry barriers, advances trade and intensifies competition within and across sectors, constantly redefining the landscape of industries as well as challenging policy silos. Continuous automatisation of various tasks and processes – part of a broader shift towards knowledge economies –- is exerting significant stress on traditional labour markets.

The pace of innovation has reached the stage where not only blue-collar jobs are being eliminated but also more knowledge-based occupations are entering long-term structural declines. In addition, our existing educational system is unable to match the demand for people with new skills (e.g. data specialists) that are replacing those in occupations that are more traditional.

Information and communications technologies are the drivers of these transformational changes. Hyper-connectivity is built by the technology companies worldwide and is testing the very definition of a technology company. If you hear automobile industry executives speak about cars these days one might think that these are just terminals on wheels. Healthcare companies speak about data and banks about cybersecurity. From banking to consumer to energy industries companies the world over are thinking digital first.

Wherever in the past tech companies were the disrupters of various business models and the transformational force in other industries, we have now reached a point where other industries are becoming the disrupters of more mature digital business models.

This shift is reflected in our collective consumer mind. According to the latest report from Interbrand[109], 8 of the top 10 brands are ICT companies. Half of the brands in

[109] http://www.interbrand.com/en/best-global-brands/2013/Best-Global-Brands-2013.aspx

the next ten are household names that helped us shape today's technological landscape. The total value of those purely tech brands in the top 20 is more than a trillion dollars. If they were a country, that country would comfortably take its place in the G20.

In 2014, three top publicly traded companies by market capitalization are also ICT champions. In the latest Fortune list of most powerful people six out of the top twenty come from the tech sector; eleven are political or religious leaders; with CEOs from the financial, retail and energy sectors making up the remaining three spots[110]. It will be interesting to see what the 2015 list looks like.

Our complete reliance on cyberspace for daily activities is now entrenched. Hence, our preoccupation with the risks it brings as well as the fear of it becoming inaccessible. A foreign concept just a few years ago, cyber resilience is now a regular discussion point during board meetings, political debates, and bar and household conversations worldwide. The world is learning that everything connected can be hacked and that it is not about being one hundred percent secure all the time but rather about being agile and resilient in order to be able to function under adverse circumstances.

Speed, mobility and collaboration are key characteristics of a successful enterprise in the digital age. To continue leveraging the benefits of hyper-connectivity, an international cyber-resilient ecosystem is urgently required. In the past couple of years, the World Economic Forum has brought together a group of executives and policymakers to explore a pathway to a more resilient digital environment. A common denominator among various ministries and industries was the concern about the dramatic increase in the number of cyber incidents in the world. If we may borrow a concept from environmental law, there is recognition that stakeholders have common but differentiated responsibilities when it comes to cyberspace, yet cyber resilience requires a high degree of multi-stakeholder collaboration. As in other areas of global governance, developing countries, which often lack nuanced understanding of cyber threats and the capacity to adequately address them, are as affected by the new risk landscape as the developed world. It is apparent that as our economies become increasingly dependent on digital connectivity, cyber resilience is emerging as a core competency for leaders in all industries or policy domains.

In response to these concerns, the World Economic Forum worked on cyber resilience by asking CEOs (as opposed to chief information security officers, chief technology officers, etc.) and senior government officials to recognise the interdependence of all

[110] http://www.forbes.com/powerful-people/list/

parties that have a role in fostering a resilient shared digital space. In doing so, we highlighted the role of leadership by encourage executive-level awareness and integrated risk management. We further encouraged a comprehensive systemic approach to cyber resilience as an enterprise expands beyond its corporate environment into the overall value chain from suppliers to customers.

The importance of cyber resilience is strongly supported by numbers in addition to public sentiment. In coming years, annual spending on cyber resilience is likely to rise, from USD 69 billion in 2013 to USD 123 billion annually in 2020[111]. These estimates of course depend on market analysis which will in turn take into account existing and projected cyber threats. Thus, in one scenario, cyber resilience investments increase 13% to USD 139 billion annually as public and private sectors improve cooperation that reflects their defensive capabilities. In another scenario, we could expect a 28% increase in spending to USD 157 billion annually if the attack capabilities and fragmented responses outpace defensive and cooperative capabilities.

Discussions of cyber risks tend to focus on doomsday scenarios or a feared “cybergeddon” and are full of overused phrases like “privacy is dead” or “weakest link”. However, equivalent concern perhaps should be the lost opportunities from a significant backlash or fragmentation of the current digital ecosystem. A backlash could result from a single major “cybergeddon” event, or through gradual erosion (death by thousands of cuts).

Fragmentation could happen at the regional, national and enterprise level and there may be many reasons why numerous actors could opt for this course of action. Thus, fragmentation could start to occur as governments concerned by the lack of a trustworthy environment are called upon to fulfil their security functions in cyberspace. Fragmentation may also start in relation to industrial policy or regulatory fragmentation in various jurisdictions.

Mckinsey estimates that the global economy might lose USD 3 trillion in potential economic growth if the increasing sophistication of attack capabilities leads to reduced investments[112]. A complex policy landscape might further complicate economic decision-making.

So what does cyber resilience look like from the perspective of an enterprise? It starts with the recognition of an interdependent, risk-based approach that presumes only

[111] http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

[112] Ibid

partial risk mitigation as a fundamental characteristic of any complex system, and an assumption that the resilience of one organisation contributes to that of the overall system.

Companies, like other organisations, attach great importance to leadership priorities. Hence the importance of involving their executive management teams and ensuring oversight governance structures like boards to develop an effective programme for cyber-risk management and for overseeing its implementation.

A set of differentiated responsibilities and shared objectives should be provided by the management team supported by necessary resources, governance, commitment and visibility of these efforts. From the standpoint of business continuity systems stress testing and "war-gaming" potential crisis scenarios, requiring coordination involving various departments from IT to public affairs, might prove very helpful should a real situation arise that would not give actors time to think through responsibilities and potential responses.

Fully integrating cyber resilience as a standard component within broader business continuity and enterprise risk management might also be helpful. A good starting point would be to identify the information assets that are mission-critical for the organisation. Defending the perimeter might have been a good strategy in the past but with the current level of attacks, probing and insider threats, the modern risk landscape calls for clear prioritization of the assets that would allow sufficient resources to be channelled into protecting them.

This would mean that all aspects of operations as well as reputational risk need to be subject to regular impact assessments. Processes should also be put in place to reduce the response time to allow for full or partial recovery in instances of major failures. It is crucial that this becomes a cross-company effort and is not viewed as purely an issue to be dealt with by the IT department.

All departments including marketing, government and public affairs, and consumer engagement, led by a top managerial team, will need to be prepared to address simultaneously restoring affected operations, mitigating potential adverse impact on the brand and customer backlash as well as potential regulatory consequences.

Many successful companies have set up a Chief Information Security Office. Some have clearly separated this function from Chief Technology Officer/Chief Information Officer responsibilities. Moreover, some have ensured that even if the positions are not of equal rank then at least their reporting lines are differentiated as strategic objectives of diverse functions that might call for different priorities in terms, inter alia, of technical architecture and acquisition.

Only by developing a comprehensive overview of the various information assets, and of the importance of an adequate, timely response to a potential breach across the organisation, can a company truly contribute to its own systemic cyber resilience. As companies put in place cyber resilience/risk-management structures, one important element to consider is compliance as governments start addressing growing insecurity with various regulatory mechanisms, from voluntarily codes of conduct to best practices, to compulsory incident reporting and standards setting.

Another important consideration is the role of suppliers, contractors and customers in the whole cyber supply chain. An enterprise should strive to raise the game among the broader ecosystem, thereby enlarging the security perimeter and making sure that coalition building occurs.

One of the most sensitive areas for international business in recent years is proactive defence. As the security perimeter becomes harder to define, a successful enterprise will leverage existing internal and external data points about changes in the threat landscape that might result in an attack. However, a large gap exists in understanding at what point the threat level crosses the internal vs. external threshold, not to mention the possibility of pre-emptive action and the issue of its legitimacy even when faced with a clear and pressing danger.

Difficulties in attribution are often cited as one of the greatest barriers, but so is the legality and legitimacy of a potential action. This grey area becomes a little more transparent in cases where a comprehensive cyber strategy at the national and enterprise levels exists, which is not always easily available. Such a strategy ought to have clear and transparent domestic as well as international components.

There has been a tremendous shift in the recognition of the problem to more nuanced understanding of the components and potential mitigation techniques among corporate leadership. Multi-stakeholder dialogue is taking place at national and international levels as the threat landscape continues to rapidly evolve.

Hyper-connectivity has already changed the way we connect with one another: it impacts our decision-making and re-organises our lives. The disruptive impact of information and communication technology is increasingly bringing about social and economic transformation. We tend to overestimate a short-term impact of technology and underestimate its long-term impact on all aspects of our lives. Cyber resilience thinking can serve as the starting point for understanding and building solutions to guide decision making to achieve the positive outcomes we all want.

2.5 The Cybersecurity Continuum to Enhance Cyber Resilience

By Solange Ghernaouti

The different dimensions of cyber resilience

Cyber-risks are a reality for everyone. Merely watching the news will convince anybody of this. Cyber criminality is a global plague and cyber attacks are now part of military doctrines. The NATO Summit of September 2014[113] defined massive cyber attacks as acts of war that could provoke a military response, and if a member of NATO were the victim, it would be considered as an attack on NATO as a whole. It is necessary to recognise that conflicts also play out in cyberspace, most commonly through cyber attacks aimed at civilian and military information infrastructures and through the manipulation of information. On the Internet, the marketing of war and of terrorism sits side by side with that of legitimate and illegal businesses, while the cybercriminal black market is doing well. The Internet has also become a popular medium for the communication of criminal activities and propaganda. Attacks on information systems can interrupt the vital infrastructures of a country, implement criminal strategies, cause losses of productivity and competitiveness, or assist the seizing of power in a country. In addition, the Internet makes easier activities designed to slow down or prevent the economic development of a country, to damage the proper functioning of a State, or to destabilise it. A great number of information systems are the targets of cyber activities aimed at destabilising a country by damaging its economy, institutions or reputation. Such activities are perpetrated in a wider context of global economic hyper-competitiveness.

Multi-faceted cyber threats are constantly evolving and it is important to understand them in an interdisciplinary and global way in order to confront them in an ongoing manner, to reinforce the security and resilience of civilian and military infrastructures, and to protect every economic actor, including small and medium-sized businesses and individuals. The ongoing process of ensuring the cybersecurity of individuals and of property, and also guaranteeing public safety, has to form part of a political project that supports a strategy of durable development for society which itself takes into

[113] http://www.nato.int/cps/en/natohq/news_112107.htm?selectedLocale=en (NATO Wales Summit Guide - Newport, 4-5 September 2014)

account its culture and specificities. This requires the involvement of all actors, private and public, and at both the national and international levels[114].

We are creating a world of permanent connectivity through mobile, wireless and contact-free[115] communications, a world where objects are becoming intelligent and able to communicate: this is the Internet of Things and of almost everything that contributes to developing smart homes and cities. Common objects such as cars and traffic lights will include IT components and Internet technologies. They will thus be capable of a certain autonomy and decision-taking, thanks to embedded intelligence in their programming. These objects are already starting to invade public spaces and are automatically becoming potential targets for malicious cyber activities because every entity connected to the Internet is hackable and can become part of botnets to attack others systems. Their security weaknesses could have damaging consequences for our physical security. While on the subject of assisting people and daily life activities, more or less sophisticated robots are starting to share our everyday existence. As these robots are capable of influencing our behaviour and our environment, their control by malicious or unwanted entities could also have negative impacts on our society. The twenty-first century is one of electronic RFID chips and nanotechnologies – the idea of intelligent dust. The convergence of the electronic and biological worlds is more and more a reality, notably in respect of the human body and the various sensors, prostheses and other elements of biomedical electronics that can be implanted in the human body to address some of its weaknesses (e.g., insulin pumps and pacemakers). Already existing neuronal interfaces allow interaction with computers via thought. If all of this can contribute to well-being, as their use and electronic and biological convergence becomes greater and more intricate, the hijacking of their initial purposes could lead to cases of hacking, including that of human thought. These new risks force us to reinvent security in order to better manage them and preserve our values endangered by the increased impact of technologies on society.

Cyberspace has become an element of civilisation upon which we rely heavily. It has thus become important that its infrastructures are robust and resilient in respect of all kinds of incidents. The concept of cyber resilience covers several dimensions which can be broken down into operational measures such as, for example, the fight against cyber criminality, the complementarity of activities related to cybersecurity and cyber defence, the effective management of energy and ecology-related risks, and the

[114] « Cyberpower: crime, conflict and security in cyberspace »; S. Ghernaouti, EPFL Press 2013.

[115] Contact-free refers to NFC (*Near Field Communication*) technologies.

education and maintenance of the human competencies necessary for the future of the information society.

Combatting Cybercrime

It has become a pressing international concern to be better prepared to combat cybercrime. No State, organisation, or Internet user is shielded from cyber nuisances, be they criminal or simply an irritation.

Being better prepared to combat cybercrime assumes that one is already prepared at some low and inadequate level. For institutions, this could take the following form:

- Having the means (i.e. strategies, measures, resources, skills) needed to address the issue, but not at sufficient quantitative and qualitative levels;
- Having the means of protection, but not at the required levels of efficiency or appropriateness.

Even if these two situations are common, it is still necessary to note that for many actors such as small and medium-sized businesses and individuals, and for many infrastructures and objects connected to the Internet, there are no control structures or security measures in place.

For a State, combatting cybercrime is based on a number of assumptions:

- Possessing a legal framework applicable at a national level compatible with international structures;
- Having judicial structures and police forces that possess the appropriate resources and competencies to function at a national level and cooperate with an international network in order to combat transnational cybercrime.

At the international level this assumes that the international community will unite around this common cause of fighting cybercrime, and that a culture of digital paradises from where the dishonest can act with complete impunity does not exist.

This situation would be to the benefit of criminals who:

- See in the Internet as a medium for committing economic crime and a tool for carrying out criminal acts (human trafficking, drug trafficking, money laundering…)
- View cyberspace as a protective layer and a global playing field.

Fighting criminality has always been a complex matter. Cybercrime has reinforced this complexity and increased the difficulty of combatting it, whether nationally or internationally.

Meanwhile, the exploits of cybercriminals are regularly recounted in the media, but do not appear to not appear to have been accompanied by sufficiently effective measures to limit the growth in power of the cybercriminals, or reduce the number of victims; there are still very few arrests and trials, compared to the proliferation of malicious activities, and this leads to a limited sense of justice on the part of the victims.

In spite of this there have been two major advances in action by States to combat cybercrime: One at the European level with the creation in 2013 of Europol's European Cybercrime Centre (EC3) at The Hague[116];

- One at the international level that led to the opening, in 2014, of the Interpol Global Complex for Innovation in Singapore[117].

Fighting effectively against cybercrime requires a preventive approach that makes cyberspace less attractive as a medium for criminality and reduces opportunities for criminal activity. Consequently, it is necessary to make cyber attacks more difficult to carry out, thus increasing the costs in terms of skills and resources, thereby reducing anticipated profits and increasing the risks for the criminals of being identified, located and prosecuted. Overall, enforcing resilience can be achieved through the following actions:

- Reducing the number of technical, organisational, legal and human vulnerabilities;
- Reinforcing the robustness and resilience of information infrastructures through technological, procedural and managerial measures that are coherent and complementary;
- Developing a real capability to adapt cybersecurity and cyber defence means to a constantly evolving situation;
- Possessing the means to manage cyber crises;
- Fighting against cybercrime monetisation circuits.

The new realm of cyberspace is filled with all kinds of activities. It is an instrument at the service of economic profitability and a place where power can be exerted: it is, in fact, a strategic territory. Thus, it needs to be protected and defended both in terms of the economy and national security.

[116] https://www.europol.europa.eu/ec3

[117] http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation

Guaranteeing the security-defence continuum in order to ensure a certain level of stability

Controlling cyber risks falls within a context of ferocious and permanent economic competition (almost economic war), the search for immediate profit, the international monetary crisis, generalised disorder, social injustice, ecological risk, and a certain deficiency in global governance. Cybersecurity should not be viewed solely in a reactive logic context aimed at "surviving" a cyber incident, whether deliberate or accidental. Although this ability to resist is fundamental and absolutely necessary, it cannot replace the absence of a multi-player global approach at both national and international levels, or a real understanding of the whole phenomenon of cyber criminality and cyber conflict. A global, interdisciplinary and integrated approach to cybersecurity and cyber defence would enable both appropriate preventive and reactive measures to be taken whose effectiveness would depend on their comprehensiveness and consistency both from a civil and military perspective. It would be utopic to think that we could respond to cyber issues without multiple levels of cooperation between many actors both inside and outside national boundaries, with the objective of supporting strategies for peace in cyberspace and in the physical world.

It may in some cases be necessary to reinvent civilian-military cooperation and dialogue to provide a coherent continuum of security defence for society at large. Cybersecurity can only be grasped in a trans-disciplinary and holistic way. At a national level, this means a shared and transversal vision of the problem, reinforced inter-ministerial cooperation, and the ability to work together.

Whatever the key purpose of a cyber attack, whatever its target (a person, an organisation, a State), the tools employed are identical. The nature and scale of the impacts vary according to the target and the motivations of the attackers, but the methods and tools in use remain the same. For a country, ensuring public safety, economic security and national security all fall somewhere along a continuum of civilian and military security. This is why it is so important that this is reflected in national cybersecurity and cyber defence strategies, in order to optimise the effectiveness and efficiency of the measures undertaken, and to respond in the best possible way to the needs of the population, both in times of peace and war. At the same time, the protection of critical infrastructure can never be a matter for either the private sector or the public sector alone – an element that also justifies the need for a security defence continuum.

It is important to protect and defend both the digital assets and heritage of individuals, organisations and States and the infrastructures that support both these assets and critical functions. This requires complementary protective measures, including activities corresponding to both the civilian and military senses of the term "protection", aimed at safeguarding infrastructures and assets that are vulnerable to cyber threats.

Developing a culture of cybersecurity and cyber defence while promoting international dialogue on these questions should contribute, in this complex and uncertain world, to a certain level of confidence and stability, on condition that every stakeholder behaves honestly and with collective responsibility. Taking into account the need to manage energy and ecology risk.

Among the indirect risks introduced by digital societies and extensive uses of information systems that have huge impacts on our planet, we should not forget, within a long-term vision of cyber resilience, to develop measures that will ensure our durability in terms of energy availability and preservation of natural resources and the ecological environment for future generations.

Therefore, we should focus in particular on risks related to:

- The elimination and recycling of electronic waste;
- The consumption of energy (growing and permanent requirements for electricity);
- Climatic warming (heat escape and the need to cool computers and server farms);
- Exploiting rare earths and metals needed for constructing electronic equipment;
- The environmental consequences of cyber attacks against systems controlling purification sites, the production and distribution of toxic products, fire alarms, etc.

Cyber resilience activities should also meet the requirements for the protection of critical infrastructure, most notably the vital elements relating to energy and the environment.

Having a proactive approach to better anticipate threats, manage cyber risks, detect anomalies to limit their impacts, and to develop cyber resilience is, from an ecological perspective, a collective responsibility. Guaranteeing education and building human capacity.

Doctrines and postures in respect of cybersecurity rely on people trained in cybersecurity issues related to several disciplines within social or technical sciences, a stance that assumes that such educational paths exist. Without cybersecurity skills and competencies across the globe, and the transfer of knowledge and cooperation to build human capacities, it will be difficult to develop behaviours compatible with cyber confidence. Good IT practices and cyber-risk awareness training are important but insufficient if the concept of cybersecurity is not integrated into products and services right at the beginning of the design phase; or if the police and justice systems are not capable of carrying out their functions because of a lack of skills; or if the political and economic players, like all Internet users, from the youngest to the oldest, do not possess the necessary skills, knowledge and experience. It is not sufficient to make populations aware of the dangers inherent in the Internet and of the elementary precautions to be taken, or to leave them solely responsible for a situation that in the vast majority of cases they are incapable of controlling. In reality, it would be unfair to make the end user and the citizen bear the cost of risks not addressed by those who created them and thereby transfer a problem for society onto people who do not by themselves possess the required remedial know-how or means.

Cyber resilience as a new challenge within cybersecurity

Resiliency to criminality is a part of a global vision of cybersecurity and contributes towards creating cyber confidence. Today it is urgent to reinforce the robustness and resilience of our infrastructures through appropriate technological, judicial, organisational and procedural measures. As with all security activities, the struggle against cyber criminality, cyber abuse and cyber misuse is complicated. This combat has to be situated within a perspective of the protection of persons and tangible and intangible assets, and defending common, broadly accepted democratic values. It is therefore useful to be in a position of possessing an efficient and effective approach to cybersecurity and cyber resilience.

To avoid the information society becoming a domain of mistrust and surveillance, it is necessary to provide convincing responses to the need to build confidence and resilience in cyberspace and to propose practical solutions for the protection of digital assets and infrastructures. Any attempt to restrict the downward spiral of cyberspace in this regard will require political will at national and international levels, resources and skills, organisational structures and procedures, and well-adapted coordination. Whether this is for legitimate or dubious actors, the new factor of the stability of societies forms part of their security and is linked to their ability to control cyber-risks and maintain cyber-nuisances within acceptable limits. Cybersecurity should not be an instrument of domination and of exerting the power of states, but an instrument of stability and of the development of peace[118].

Chapter III: Cyber Freedom

Introduction

While the previous chapter stresses the crucial importance of building cyber resilience to ensure a cyberspace inspiring confidence, this final chapter presents an overview of the challenges of cyber freedom and emerging related threats from both the public and private sectors that undermine the hope of achieving Internet freedom.

Freedom of opinion and speech, free access to information and the right to privacy have always been central elements of civil society as they reflect fundamental human rights and civil liberties that underpin democratic principles and values. The emergence of the Internet and Information communication technologies have given billions of people around the world opportunities to access hitherto unimaginable amounts of information and means of communication. Indeed, they represent vast platforms for the exchange of opinions, data and innovative ideas. At the same time, however, these essential tools of the digital age are also being exploited to undermine progress, political rights and privacy, thus eroding confidence in their use.

As the European Court of Human Rights has emphasised on many occasions, “Freedom of expression [...] is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population."[119]

Although blogs and social media have opened up new opportunities for exchanging ideas, in recent years certain States have resorted to Internet blocking as a new extension of government censorship aimed at controlling public opinion and undermining freedom of information and expression.

[118] Enforcing cyber confidence at a global level will contribute to resolving the main cyber peace issues raised as those highlighted in “The Quest for Cyber Peace” – ITU 2011 (http://www.itu.int/pub/S-GEN-WFS.01-1-2011)

[119] European Court of human Rights Case of Handysive v The United Kingdom http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["695376"],"itemid":["001-57499"]} last updated on 17/10/2014

This challenges the advantageous features of the Internet which are its boundless all-pervasiveness and its worldwide accessibility by raising the current debate about net neutrality highlighting the problem of guaranteeing equal rights to access this essential medium of our time.

The massive extent of highly available data characterizes today's information society and accentuates emerging threats of espionage from both public and private sectors thus endangering our right to privacy and safe use of digital tools. In fact, in order to ensure national security, governments justified surveillance can rapidly lead to massive data collection and storage of personal information making it difficult to draw a distinction between acceptable and unacceptable practices perceived to cross a red line.

At the same time, to benefit from the most convenient data protection regime, in the quest for financial and competitive advantage, the private sector collects and transfers vast amounts of personal data across borders, thereby bringing in new risks to personal data.

Given the borderless nature of the Internet, national laws are not sufficient to ensure Internet freedom. That is why it is so essential to elaborate and adopt an international framework to build cyber confidence.

This chapter is divided into five sections. First, it underlines the lack of an adequate legal framework that impacts the protection of civil liberties in cyberspace and Internet freedom, as illustrated by the current situation in many parts of the Arab world. It then highlights the debate around Big Data and the issue of data protection in order to underline the need for an international regulatory framework to preserve Internet freedom and the right to privacy. The third section deals with the topic of State surveillance and intelligence gathering in cyberspace and their impact on efforts to build confidence in the use of cyberspace.

The fourth section discusses the European perspective pertaining to government encroachments of digital privacy and data protection, and the importance of a harmonised policy in this regard within the European Union, not only to facilitate cooperation among its Member States but also to serve as an example beyond its borders. Finally, the last section undertakes to establish criteria for the management of cyber freedom as a fundamental human right and a powerful agent in building cyber confidence.

3.1 Cyber Freedom: Progress and Challenges

By Mona Al-Achkar

Introduction

The power of new technologies has heralded an era that is increasingly brushing aside the technical constraints of what can be done at multiple levels, a digital age in which individuals and nation States are empowered as never before, not only to develop, but also to project great abuse and violence.

This paradox is reflected in the undeniable benefits of the digital age when set against the manifold dangers faced by individuals, the business world and nation States stemming from the increasing reliance on ICTs and the mounting and ever more sophisticated criminal activities in cyberspace. Threats to national security have become more acute, and critical infrastructure is increasingly exposed to multiple risks, including attacks via the Internet.

Alongside cybercrime, incompatibility and the absence or lack of a legal framework are still the major factors undermining confidence in the use of cyberspace platforms. This is because they allow the establishment of legal insecurity, and hinder the full exercise of civil liberties. Consequent, policing of the Internet poses a real threat to many civil liberties such as privacy, freedom of expression, protection against self-incrimination, unwarranted searches and seizures, and the right to due process of law. The protection level of these civil liberties largely depends on the legislation, legal practices, and political system in place in a given country or region.

Protecting these civil liberties and thus building confidence in cyberspace is an essential prerequisite to ensuring a trustworthy economic cyber environment. This was clearly illustrated by the PRISM affair, which revealed clandestine personal data collection and spying operations by the US National Security Agency. Following this disclosure, Cisco declared an 8 to 10% drop in revenue, and predicted more decreased activities and lower income for 2013-2014, due both to the world economic situation and the impact of the PRISM scandal.

Such mass surveillance, combined with emerging concepts of “cyber repression” and “electronic police States”, point towards a decline in many of the aforementioned civil liberties, both in dictatorial regimes and in democratic countries.

Civil Liberties

The term "civil liberties" comes from Latin ("ius civis"), which means "rights of citizens" and derives from the Magna Carta designed to limit abuse of power by the authorities. That is why civil liberties are acknowledged as protective against illegal practices and acts by governments and their violation of basic legal rights.

Whereas human rights are universal and apply in equal measure to all countries, civil liberties relate to the national legislation of each country. Accordingly, each country grants its own citizens the basic freedoms granted under their respective national legal systems. The main importance of civil liberties is that they restrict the level of State interference in the lives of citizens, as well as all forms of abuse of power and thus ensure the ability of citizens to participate in the civil and political life of the country, without being subjected to discrimination or repression.

Civil liberties include personal, political, and economic rights such as: the right to a fair trial, the right to due process, freedom of association, the right to petition, the right of self-defence, the right to vote, freedom from slavery and forced labour, freedom from torture and death, the right to liberty and security, freedom of conscience, freedom of religion, freedom of expression, freedom of speech, the right to privacy, the right to own property, the right to marry, the right to defend oneself, the right to physical integrity, the right to use facilities, the right to an equal education, and the right to participate in public function.

Civil liberties established by domestic laws may have a common legal base such as the civil liberties' tort, which allows individuals to seek compensation – not only from other individuals but also from the government – when wronged or injured through violation of their basic rights. Such violations would include for example unwarranted intrusion into a home or one's privacy, defamation, or illicit appropriation.

Freedom of information: The right to access information

Freedom of Information or the right to access information has emerged as a new right, distinct but inseparable from the right to freedom of expression. It can be defined as the right to access information held by public bodies[120].

According to the final document issued by an experts' meeting organised by the Commonwealth Secretariat, which took into account Article 19: "Freedom of

[120] http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/

information should be guaranteed as a legal and enforceable right permitting every individual to obtain records and information held by the executive, the legislative and the judicial arms of the state, as well as any government owned corporation and any other body carrying out public functions."

The basic principle behind this freedom resides in the right of citizens to know, the obligation of governments to inform its citizens, and in the fact that the burden of proof falls on the party to whom the information request is addressed. That is why most governments tend to classify information they do not wish to disclose as secret or withhold it for *raisons d'état.*

The right to access information includes the right to seek, receive and impart information and ideas, and covers both those who actively seek information as well as those who expect to receive it through the media or official channels. This right mostly relates to access to public information. It underlines the principle of publicity of acts, as well as public administration transparency, which makes its application directly related to the active participation of citizens in political life, and in mechanisms to counter corruption.

According UN General Assembly Resolution 59 (1): “Freedom of Information is a fundamental human right […], “the touchstone of all the freedoms to which the UN is consecrator”[121]. Similarly, the preamble of the Lima Principles or the Chapultepec Declaration affirmed that “[…] the individual right to freedom of expression and access to information are fundamental to the existence of all democratic societies and essential for the progress, welfare and enjoyment of all other human rights”.[122]

Moreover, in its Tunis Commitment, the World Summit of the Information Society reaffirmed the need for nation States to respect human rights and fundamental freedoms, and recognised the importance of “[…] freedom of expression and the free flow of information, ideas, and knowledge in information society”.[123]

The right to access information is therefore considered as fundamental to the exercise of *inter alia* freedom of expression and liberty of belief. It involves the obligation of governments to guarantee the free flow of information and ideas. Abid Hussain, the then UN Special Rapporteur on Freedom of Opinion and Expression, stated in his 1995

[121] UN General Assembly, (1946) Resolution 59 (1), 65th Plenary meeting http://foishehri.wordpress.com/

[122] http://www.rjionline.org/MAS-Codes-Peru-Lima-Principles

[123] - http://www.itu.int/wsis/docs2/tunis/off/7.pdf

Report to the UN Commission on Human Rights: “Freedom will be bereft of all effectiveness if the people have no access to information. Access to information is basic to the democratic way of life. The tendency to withhold information from the people at large is therefore to be strongly checked."

Levels of freedom of access to information vary from country to country. Some recent developments are particularly noteworthy in this regard. For example, a recent post-Arab Spring development in some Arab countries was the inclusion in their constitutions[124] of a provision guaranteeing the right to information[125]. In another indicator, the US Patriot Act makes it more difficult for American citizens to access information from their government.

While nation States are asked to recognise and respect this right, it should be pointed out that it is often restricted by authorities whenever it is deemed to hamper or compromise the protection of national security, territorial integrity, public safety, crime prevention, protection of health or morals, and other individuals' privacy, reputation or rights. These restrictions should however be decided according to the law, and to the requirements of preserving judiciary impartiality and the proper functioning of democracy.

In cyberspace, freedom of information empowers individuals and organisations to exercise greater levels of free expression and social exchange. At the same time, it raises a new set of challenges that may restrict social media usage. The Arab Spring and the WikiLeaks stolen documents are the most recent examples. Apart from the challenges such cases pose to national interests and the secrecy of classified data, they also highlight restrictions and policing practices on the Internet by both States and private sector entities.

Building on the G8 commitment of 2004 to promote an environment conducive to an informal, flexible, open and inclusive dialogue, the Middle East and North African countries launched an initiative called The Forum for the Future later the same year. Subsequently, in July 2008, Arab civil society organisations from Bahrain, Egypt, Jordan and Morocco established the Arab Freedom of Information Network. But despite ongoing concerted advocacy in the region, legislation on freedom of information has made no progress in most Arab countries. Jordan and Tunisia are still the only Arab

[124] http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

[125] http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

States to have enacted an Access to Information Law, although bills in this regard have been debated in Bahrain, Egypt, Kuwait, Lebanon, Morocco, Palestine and Yemen. In Lebanon, in 2004, a draft law on "whistle-blower protection" was prepared by a group of Lebanese lawyers, assisted by the American Bar Association, and submitted to the Lebanese parliament in 2010 by the National Network for the Right of Access to Information in Lebanon.

Privacy: Protecting against the World Intelligence Community

Privacy is a civil liberty directly related to personal freedoms, dignity and integrity. It resides in the right of citizens to protection from unwarranted government interference in their lives such as unauthorized home searches and correspondence/communication eavesdropping. In the digital age, privacy is considered in a new context. It is no more confined to protection of the physical and material environment, such as the home, mail or documents, but now extends to the huge volume of personal data in cyberspace, and to the high level of connectivity that is turning each individual into a "sensor for the world intelligence community".[126]

There is no global consensus on what can be considered as adequate protection of privacy. Nonetheless, there is a basic international legal framework for the right to privacy, which can be extended to cyberspace, and which reflects the provisions of international, regional and national legislations, declarations, conventions and treaties.

Article 12 of the Universal Declaration of Human Rights recognizes privacy as a fundamental human right. According to this Declaration, no one shall be subjected to arbitrary interference in their privacy, family, home or correspondence, and everyone has the right to legal protection in this respect.

Article 17 of the International Covenant on Civil and Political Rights reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to unlawful attacks on his honour and reputation, and, consequently, everyone has the right to the protection of the law against such interference or attacks."

[126] Philippe Langlois- founder of the Paris-based company Priority One Security, on agencies' ability to harvest personal data from users of smartphones.

http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

Among other relevant guidelines, conventions and directives are:

- The 1980 “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” issued by the Organisation for Economic Cooperation and Development.
- The 1981 “Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data”, issued by The Council of Europe (CoE).
- The 1989 “Guidelines on the Use of Computerised Personal Data Flow”, issued by the Council of Europe.
- The 1999 UN “Guidelines for the Regulation of Computerized Personal Data Files”.

These instruments establish principles of minimum privacy guarantees for personal information at all stages of its processing (collection, storage, dissemination, use, transfer etc.). They also recognise the right of the individual to access h/her personal data, to update it, and to be informed on the methods and the objectives of data collection operations. Moreover, they establish the right of the individual to have his data destroyed, after the purpose of its collection and processing is established, which supports the right to be forgotten on the net. At the regional level, some countries have already set measures and minimum levels of adequate protection relevant to privacy issues.

The 1995 EU Data Protection Directive allows collection of personal data for specific, explicit and legitimate purposes, and prohibits holding any data that is not up-to-date, relevant and accurate. Furthermore, EU Member States are obliged to stop transfer of this data abroad[127] in the absence of equivalent measures that allow data protection and citizens‘ rights to access, protect, modify, and deny the right to use of their data by a third party.

For example, to allow transborder data flow to the US, where no such level of adequate protection is in place, the EU reached the “Safe Harbour Agreement” with that country. This agreement allows some US companies to collect data about EU

[127] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - *Official Journal L 281 , 23/11/1995 P. 0031 - 0050*

- (57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

citizens, on condition that they prove their engagement to ensure that this data is protected in accordance with EU standards. Moreover, these companies are required to inform the EU citizens concerned how their data are processed and used, and to recognise their rights to access, withhold, and modify it.

At the regional level, the EU Data Protection Directive regulates the free movement of personal data between its members, and imposes the adoption of its provisions into domestic law, while allowing individual EU countries to exercise their own approaches to implementation. Data subjects must be guaranteed the right to know where the data originated, the right to have inaccurate data corrected, the right of appeal in the case of unlawful processing, and the right to deny permission to use data under certain circumstances.

At the domestic level, almost all countries recognise a constitutional right to privacy. Some new constitutions (South Africa) and many European countries have approved laws to regulate surveillance of personal data and protect citizens' privacy[128]. The UN has supported privacy protection by endorsing a draft resolution[129] prepared by Brazil and Germany, and titled "The right to privacy in the digital age."[130]

Freedom of expression: Hallmark of democratic society

In democratic societies, legislations, free speech and independent civil society are the protectors of freedom and civil liberties, as opposed to the hallmarks of tyrannical regimes such as police impunity, unfair trials and arbitrary detention.

According to Article 19 of the Universal Declaration on Human Rights, as well as to Article 19 of the International Covenant on Civil and Political Rights, "Everyone has the right to freedom of opinion and expression. This right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas

[128] FISA Amendments Act of 2008, Communications Assistance for Law Enforcement Act, in the USA

- Data Protection Act 1998 and Regulation of Investigatory Powers Act (RIPA) in the United Kingdom - Informatics and civil Liberties Act 1978 in France - EU convention of Personal Data Protection, EU Data Retention Directive,

[129] General Assembly backs right to privacy in digital age.

http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

[130] Sixty-eighth session- Third Committee- Agenda item 69 (b) Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms.

through any media and regardless of frontiers." Freedom of expression means being able to freely express ideas and beliefs on economic, political, social or other subjects via all available means of communication – e.g., writing, painting, broadcasting, or blogging. Accordingly, freedom of the press and freedom to use social media are part of this freedom.

Likewise, Article 11 of the EU Charter of Fundamental Rights, corresponding to Article 10 of the European Convention on Human Rights, reads: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. Further, it states: "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary." Moreover, as with all restrictions of rights and freedoms, it recognises the principles of necessity and proportionality, and that of the need to refrain from arbitrary or discriminatory practises.

Accordingly, freedom of expression is considered elemental in achieving citizens' confidence in their government and the political system, allowing for implementation of other human rights, better understanding of public policies, the creation of well-informed public opinion, and freedom to voice concerns through the media. At national level, freedom of expression is recognised in many constitutions as a hallmark of democratic regimes. In this context, the UN General Assembly considers that monitoring of telecommunication networks threatens human rights and many civil liberties, ranging from freedom of opinion and of expression to the right to privacy and political activism, and that it undermines the foundations of a democratic society[131].

Thus, freedom of expression online is to be respected and governments are expected to refrain from stifling it and should remove any obstacles in this regard. In particular,

[131] UNGA- 16 May 2011 A/HRC/17/27- Human Rights Council- Seventeenth session- Agenda item 3 - Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development "The growing use and sophistication of digital surveillance has outstripped the ability of societies to legislate their proper use, leading to "ad hoc practices that are beyond the supervision of any independent authority," and that threaten to repress free expression".

for the purpose of our presentation, they are expected to refrain from cyber repression that silences opposition voices, and from interception of communications, content censorship, or blocking websites.

In reality, however, freedom of expression is not respected in many countries. Some governments evoke the protection of religious values and decency, in addition to national security and the combat against terrorism as reasons for restricting freedom of expression online. They censure content they may consider sexually explicit, or that promotes hate on the basis of race, religion, or other cultural factors, or that encourages terrorist activities. The danger resides in the legal terminology used to reprimand such content, which in general is expandable, meaning that it may lack objectivity and stability of justice, and thus lead to abuse of authority.

Social Media

Discussion, the exchange of views and common goals, and lobbying are traditionally preliminary steps in organising protests that sometimes lead to revolution. The abundance of social media exchanges about freedom of the Internet and democracy, coupled with the growing capacity of citizens to impact national politics, played a critical role in shaping political debate during the Arab Spring. This provided an empowering new space, through blog posts, Tweets, and YouTube uploads. In the words of an Egyptian activist: “The Internet deserves the highest protection from governmental intrusion. If you want to liberate people, give them the Internet.”

Social media enables the mobilisation of people as well as clandestine information exchanges like never before. It provides great opportunities to organise and vehicle information, and can help form and structure opposition groups, recruit militants, reach out to supporters, spread ideology, and create internal as well as external support networks. During the Arab Spring, militants used social media to obtain regional and international support, and to organise propaganda campaigns.

Even though social media cannot replace the physical actions required to foment successful revolutions, it has provided Arab citizens an opportunity to use information as a potent weapon against repression. Participants in Arab Spring movements used social media to stay connected, share information, spread news about actual events, organise their activities, disseminate information and news, send messages to the world, and influence public opinion. Pictures and videos sent over mobiles helped in collecting information on government forces and their positions. Political actions were essentially organised and promoted on social networks. Before and during the Arab Spring regime changes in several Arab countries, tweets by opposition groups went viral and reached millions of viewers and Facebook pages. Blogs increased dramatically, generating discussion across the region on democracy, liberty and transparency. Millions of citizens were on social media, and many pages and sites were created to foster opposition outreach through online messages and blogs. Using their cell phones, some activists provided real-time footage of events and posted it on Facebook, Twitter and other social networks. Today, many of the slogans of that time are frequently used in different countries in various social, political or economic protests.

Worrying attacks on free expression have been very significant In Lebanon over the past year. Its reputation as a bastion of free speech has been tarnished by a rash of arrests, detentions and intimidation of Lebanese citizens related to their online activities, especially on social media.

Politicians in Lebanon seem to be increasingly on the defensive, ostensibly challenged by 140 character tweets and other social media content. For example, four Facebook users were arrested and one Twitter user was sentenced to two months imprisonment for insulting the President of the Republic. In another case, a blogger held in detention for more than eight hours was threatened with prosecution unless he stuck to writing poetry rather than politics. Several bloggers have been questioned by the cybercrime authorities and some blogs blocked, among them a post about unfair treatment of workers at a major supermarket chain.

Such rulings, akin to sanctions in autocratic countries, have been uncommon in the past in Lebanon, where expression of opinion has been relatively unregulated in the past.

Dangers: Facts and Actors

Cyberspace represents the new dimension of national security and is a precious mine of information for intelligence gathering. But the traditional ways of monitoring and collecting information by security entities are no longer adequate.

Today, there is a need to identify and target plotters and to anticipate the actions of networks that may be malicious and criminal. For this purpose, sophisticated technologies are being deployed for mass surveillance of computer networks and users, to detect, identify and trace intruders, and to preserve evidence-based data.

The collection of personal data and associated abuse of civil liberties are making headlines in the media across the globe; the Snowden, WikiLeaks and Tempora[132] disclosures, amongst others, have led to a tightening of the grip on the net through SORM-2 and SORM-3[133], single register[134], and social network censorship[135]. Recently, some governments increased Internet controls through measures to ensure online user identification[136].

Personal data may be accessed by security agencies and checked against lists of intelligence targets. Surveillance technologies allow them to pinpoint the location of targets using Google maps or movement-tracking GPS systems, or components that are embedded in pictures posted on social networks. Using such technologies they can also obtain address lists and telephone records of family members and friends by recording and storing emails. According to secret British intelligence documents, spies are even lurking in the background of popular game applications to obtain data revealing the location, age, sex and other personal information of players.

This phenomenon greatly fragilises privacy and many civil liberties. But the challenges to our privacy and other civil liberties do not come from governments only. Illegal surveillance of individuals is conducted both by public and private actors because it can useful both for marketing and intelligence gathering. Corporations large and small

[132] Tempora, is a clandestine security electronic surveillance programmer tested in 2008,[2] established in 2011 and operated by the British Government Communications Headquarters (GCHQ). Tempora uses intercepts on the fibre-optic cables that make up the backbone of the internet to gain access to large amounts of internet users' personal data. http://en.wikipedia.org/wiki/Tempora

[133] - These laws seem to be in conflict with Article 23 of the Constitution of Russia which states:[32]

1. Everyone shall have the right to the inviolability of private life, personal and family secrets, the protection of honour and good name.
2. Everyone shall have the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages. Limitations of this right shall be allowed only by court decision.

[134]In Ex-Soviet States, Russian Spy Tech Still Watches You- By Andrei Soldatov and Irina Borogan- 12.21.12 6:30 AM

http://www.wired.com/dangerroom/2012/12/russias-hand/all/

[135]King, Gary, Jennifer Pan, and Margaret Roberts. 2014. Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation. Copy at http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

[136] China orders real name register for online video uploads.

http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121 track what we buy, compile personal data to send tailored ads to people's mobile phones, store and analyse data, and use it for commercial purposes. They sometimes collect particularly sensitive data they label as optional pertaining, *inter alia*, to ethnicity and sexual orientation.

Government censorship is being applied through measures such as Internet filtering, deployment of malicious monitoring tools like Trojan horse[137], and restrictions on online anonymity. These measures aim to facilitate State communications surveillance by simplifying the identification of individuals accessing or disseminating prohibited content, and to gather Intelligence.

The scale of collected data and taped communications is quite remarkable – and disconcerting – and represents a serious risk for privacy and civil liberties.

Some positive aspects of this surveillance are nonetheless evident. For example, surveillance helped foil an Al Qaeda bomb plot in Germany in 2007, and the arrest of those behind drug [138] and child pornography networks[139]. In this context, we can also mention the European INDECT project "Intelligent information system supporting observation, searching and detection for security of citizens in urban environment", which aims to ensure the security of citizens, mainly in relation to violence.

Focus on the Arab World[140]

Most Arab countries are members of the UN, and all are members of the League of Arab States, composed of independent Arab States in north and northeast Africa and southwest Asia. The purpose of the League is to strengthen relations between member States, to foster cooperation among them, and to safeguard their independence and sovereignty. More specifically, it aims to cement close cooperation in the economic, financial, communications, health, social and cultural domains, and in

[137] The QQ application in China which is considered as a giant Trojan horse.

[138] Drug lord Guzman arrested. http://news.yahoo.com/internet-crucial-venezuela-battleground-075124059.html

[139] How the NSA's High-Tech Surveillance Helped Europe Catch Terrorists.

http://www.civilbeat.com/articles/2013/06/21/19341-how-the-nsas-high-tech-surveillance-helped-europe-catch-terrorists/

[140] The Arab world is here defined as the members of the Arab League: Algeria, Bahrain, Comoros, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, Palestinian territories, Qatar, Saudi Arabia, Somalia, Sudan, Syria (suspended), Tunisia, United Arab Emirates, and Yemen.

matters pertaining to nationality, passports, visas, execution of judgments and the extradition of criminals.

Arab countries are committed to respect freedom of expression, according to Article 19 of the Universal Declaration of Human Rights, and to Article 32 of the Arab Declaration of Human rights modelled on the aforementioned Article 19.

Social mores and traditions, as well as religion are generally the declared reasons for restrictions and repression. Some countries have adopted emergency laws, which are always intended to stifle dissident opinion by prosecuting those who dare to speak their mind freely. They could be victims of brutal arrests, torture, and imprisonment for the crime of belonging to an “illegal organisation”, treason, or for plotting against national security and interests. Some governments are establishing or enforcing their capacities to restrict civil liberties through the use of blue-coat proxies and foreign technologies to track and block dissidents’ communications.

Online censorship is extensive, although governments claim they only censor pornographic sites. Users may find themselves directed to a proxy server that maintains a list of banned websites and blocks material deemed inconsistent with local religious, cultural, political and moral values. Most journalists and bloggers practice self-censorship, particularly regarding issues such as local politics, culture, religion, or any other subject the authorities may consider politically or culturally sensitive. In general, they avoid criticising the Head of State or other officials, or publishing information that could potentially harm the country’s reputation, foreign relations, or national economy. Defamation is a criminal offence.

In one high-profile case in the United Arab Emirates in 2009, freelance journalist Mark Townsend, a former business editor of the Dubai-based English-language Khaleej Times, was accused of criminal defamation, and was unable to leave the country for nearly two years as the investigation proceeded. He was charged under Article 373 of the penal code for allegedly posting articles that criticised the Khaleej Times, in which the government holds a 30 percent stake, and faced a maximum sentence of two years in prison and a fine of up to 20,000 dirhams ($5,400). He was ultimately acquitted in May 2011. In another case, in 2011, five Emirati activists and bloggers were arrested and charged with insulting the UAE leaders in posts on the UAE Hewar internet forum. They received prison sentences.

On a more positive note, the Internet has developed into a space for organising and lobbying among activists. The caveat, however, is that Arab governments cut off the Internet whenever anti-government civil demonstrations break out.

Privacy in the Arab world is mainly perceived in physical and material terms. Its primary focus is on factors such as the inviolability of the home, personal correspondence and communications. Arab legal systems do not however adequately protect the right to privacy, apart from the rare cases where it is protected under the constitution or in codes.

In Lebanon, privacy does not have a well-defined legal status, although the subject has been widely debated among political leaders. It is protected by a combination of constitutional and legislative provisions. The Lebanese constitution, much like its US counterpart, does not define the right to privacy. Nonetheless, it safeguards the protection of the person and that of a person’s residence and personal effects.

Some provisions protect people’s personal lives from exposure under certain specific circumstances. Article 17 states that the place of residence is inviolable and that no one may enter it except in specific circumstances and in line with conduct defined by law. Moreover, an eavesdropping law states that citizens are entitled to the privacy of their local or international wired or wireless communications means.

The Lebanese constitution recognizes the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, which may only take place wen authorized in conditions prescribed by law. Following the example of many governments around the world, in Lebanon, the legal basis for justifying invasion of privacy, compromising many civil liberties in the process, is always built around pretexts such as national security, curbing terrorism, and protecting public welfare.

Similar pretexts are given to justify government blockages of Internet-based social media sometimes used to promote and organise protest activities in the Arab world.

In March 2013, Reporters Without Borders labelled several Arab countries "State Enemies of the Internet"[141] because of their practices such as crackdowns on bloggers, resulting in grave violations of freedom of information and human rights.

[141] Reporters Without Borders' March 2013 – Special report on Internet surveillance, titled "Enemies of the Internet “focusing on 5 governments and 5 companies. http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html

The League of Arab States and civil liberties

The League of Arab States was established seven months before the creation of the United Nations by six countries (Egypt, Iraq, Lebanon, Saudi Arabia, Syria, and Transjordan) and now has twenty-two Arab States members.

The charter that established the League in 1945 made no reference to human rights. Moreover, there is no specific provision for the protection of human rights defenders in Arab League legal documents.

On the other hand, the League formed a committee to work on achieving a more integrated and harmonized legal system, by unifying legal and judicial terms, structures and processes. To implement the recommendations of this committee, the League established the Arab Center of Legal and Judicial Studies in Beirut. This Center has elaborated numerous conventions related to Arab country cooperation on many legal issues of common concern, such as the cybercrime legislation model. It cooperates with many international and regional organizations as well as with civil society bodies on Internet governance issues. For example, it worked with UN-ESCWA to establish and inaugurate the Arab Internet Governance Forum. Alternatively, it has been a founding member of the Pan Arab Observatory for Cyber Security since 2009 and initiated the drafting of an Arab cybersecurity convention to be submitted to the Council of Arab Ministers of Justice. The draft clearly mentions the protection of civil liberties on the Internet as a vital element to build confidence in the use of cyberspace. At the same time, the Center has inaugurated many forums and annual meetings for ICT decision makers on issues related to human rights and civil liberties, in particular the rights to privacy, access to information, and freedom of expression.

Conclusion

Concerted legislative efforts are needed to establish an appropriate balance between the need to protection civil liberties, Internet user privacy, and, first and foremost, freedom of expression, against the need to counter cyber threats to national security. Success in this respect would serve to prevent cyberspace from becoming a new domain for surveillance.

States must prosecute cyber offences as crimes under national law, which should combine proactive and reactive measures to protect civil liberties. A dedicated international treaty or agreement providing for a reasonable minimum level of protection acceptable to all parties concerned would help safeguard privacy during information exchanges. This should be complemented by an efficient international cooperation framework to combat transnational cybercrime. In this regard, the Centre for Legal and Juridical Studies at the League of Arab States has requested me to prepare a draft Arab convention on cooperation to combat cross-border cybercrime.

Within this cooperation framework, investigations, tracking, prosecutions, mutual legal assistance, and judicial proceedings would need to be carried out in accordance with national laws. Similarly, any authorised international law enforcement procedures should be applied in accordance with domestic legislation and mutual legal assistance treaties. States should introduce special procedures and measures to protect international exchanges of sensitive information, and to monitor computer networks, and data collection and processing. This is a particular necessity in countries that lack an adequate level of privacy legislation.

Special attention should be paid to protection against illegal searches and seizures. The technical nature of cyberspace, coupled with growing levels of cybercrime and the absence of a relevant international criminal law framework, complicate the task of ensuring respect for civil liberties.

In most national legal systems police conduct is regulated by the constitution, legislation, and procedures that protect citizens against abusive law-enforcement powers and actions, such as unwarranted searches and seizures, and the violation of civil liberties when carrying out such operations.

As many countries still lack cyberspace laws and procedures, and refer to general criminal laws in regard to cyber issues, their respective governments could alternatively adopt guidelines aimed at preventing abuse of civil liberties in this domain. Such guidelines should notably clearly define what warrants legal searches and seizures within the limits of justified exceptions to requirements to respect civil liberties. The guideline framers could be inspired by traditional law exceptions related to “plain view doctrine”, or “exigent circumstances”.

Such exceptions could be offset by various protective measures: encryption, anonymous remailer servers, secure anonymous communications, firewalls, and proxy servers. Many of these technologies offer protection against cybercrime, coupled with enhancement of privacy.

3.2 Legal, Policy & Regulatory Frameworks for Internet Freedom & Big Data

By Pavan Duggal

Introduction

Today's dynamic world has been revolutionised by the exponential growth of cyberspace. The Internet has made geography history, yet this boundary-free medium that cyberspace has created has become a subject of immense concern for all governments across the globe. It is for this reason that the issue of coming up with appropriate policy and regulatory frameworks for cyberspace has become so critically urgent.

Internet is all based on the foundation of data and information in the electronic form. In fact, both the terms "data" and "information" are used interchangeably and both of them refer to the building blocks which are essential for creating the content architecture as also which form the foundation of communication channels riding the Internet.

The development of the Internet from the Advanced Research Projects Agency Network (ARPANET) in the late 1960s to the World Wide Web and onwards to the present age of social media and Social, Mobile, Analytics and Cloud (SMAC) has been a long journey. The Internet has been a great leveller in that it affords freedom of access to information for all users and helps facilitate their daily issues and aspects of human activities in countless ways.

Huge volumes of data are created by the Internet. Former Google CEO Eric Schmidt stated in 2010 that every two days "[…] we now create as much information as we did from the dawn of civilisation up until 2003, something like five exabytes of data". Echoing this astonishing growth, IBM says that each day we generate 2.5 quintillion bytes of data — "[…] so much that 90% of the data in the world today has been created in the last two years alone".[142.] Yet further evidence of this phenomenon is reflected in a statistic quoted in an IDC-EMC report stating that the digital universe is more than doubling every two years, and will reach 40,000 exabytes (40 trillion

[142] http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

gigabytes) by 2020[143]. The Economist reported in its 2012 Outlook that the quantity of global digital data expanded from 130 exabytes in 2005 to 1,227 in 2010, and is predicted to rise to 7,910 exabytes in 2015[144]. Concerns about these huge volumes of data have been exacerbated by the emergence of big data in the digital ecosystem.

This paper looks at the legal, policy and regulatory frameworks for Internet freedoms and big data.

Definition

Before proceeding further with an examination of the legal and regulatory issues pertaining to Internet Freedom, one should be aware of the various definitions of this term advanced by different scholars and jurists.

Defining Internet freedom is a broad and controversial subject; there is no universally agreed definition. President Obama once stated: "The Internet has unleashed innovation, enabled growth, and inspired freedom more rapidly and extensively than any other technological advance in human history. Its independence is its power. The Internet offers a communications system uniquely free from government intervention."[145] He notably added: “Internet freedom is inconsistent with net neutrality regulation and uniquely free from government intervention.”

Derek Bambauer, a professor of Law at the University of Arizona says: “Perhaps, in the end, Internet freedom is a term that should be abandoned as too general to be useful. Instead, countries, cultures, and users should grapple with the difficult trade-offs that Internet communication presents.”[146]

Here’s how “Media Marxist outfit Free Press” defines Internet Freedom on its website: “Internet Freedom means that Internet service providers (ISPs) may not discriminate

[143] http://www.baselinemag.com/analytics-big-data/slideshows/surprising-statistics-about-big data.html#sthash.COE9uzq6.dpuf last updated Aug. 4, 2014.

[144] Welcome to the yotta world’, The Outlook for 2012, Economist, Dec. 2011; http://www.economist.com/node/21537922

[145] http://freestatefoundation.blogspot.in/2012/08/the-true-meaning-of-internet-freedom.html

[146] Bambauer, D., The Enigma of Internet Freedom, eJournal USA, Vol.15, No.6, 2010, pp. 4-6., see also http://www.wseas.us/e-library/conferences/2013/Dubrovnik/ECC/ECC-38.pdf, last updated Aug. 8, 2014

between different kinds of online content and apps".[147]. Dictionary.com defines Net Neutrality as the principle that basic Internet protocols should be non-discriminatory, especially that content providers should receive equal treatment from Internet operators.

Internet Freedom means Open Spectrum

While broadcasters and mobile phone companies have government-issued licenses for certain segments of the airwaves, other frequency swaths are open, meaning that any company can develop a product — like a cordless home phone, Bluetooth headset, baby monitor or remote control — that utilises this open space without any need for a government license[148].

Internet freedom brings with it not just the freedom to access this medium but also the freedom to express oneself. But more importantly, it signifies the freedom to makes people's lives easier by making life easier given the various facilities provided by the Internet.

Salient Features

Some scholars have concluded that Internet freedom encompasses a range of fundamental freedoms such as freedom of speech, the right to privacy, freedom to innovate and to be rewarded and recognised, and freedom of the Internet architecture as a whole[149].

Existing Policy and Regulatory Frameworks

Despite the development of the Internet as a global and borderless medium, the fact remains that the world still has not yet focused on coming up with internationally accepted norms specifically applicable to cyberspace. Consequently, when one talks about the legal, policy and regulatory frameworks, it is important to note that there are no international treaties on Internet freedom. However, there are some advances in this direction.

[147] http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

[148] http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

[149] Neelie Kroes, *Internet Freedom,* http://europa.eu/rapid/press-release_SPEECH-12-326_en.pdf, Last updated Aug. 8, 2014

As mentioned earlier in this report, the 2001 Convention on Cybercrime of the Council of Europe is a prominent example in this regard. The salient features of this Convention are as follows:

- It is the first international treaty that seeks to address cybercrime by harmonising relevant national laws, providing common definitions for certain criminal offences improving investigative techniques, and increasing cooperation to the "widest extent possible" among nations to combat this phenomenon[150].
- It requires the criminalisation of such activities as hacking and offences relating to child pornography, and expands criminal liability for intellectual property violations.
- Provides a common criminal policy aimed at the protection of society against cybercrime by adopting appropriate legislation and fostering international co-operation[151].

The Declaration on freedom of communication on the Internet, adopted by the Council of Europe in 2003, is yet another striking example of these efforts. The following are the fundamental features of this Declaration:

- States need to balance freedom of expression and information with other legitimate rights and interests, in accordance with Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms;
- Expresses concern about attempts to limit public access to communication on the Internet for political reasons or other motives contrary to democratic principles;
- Asserts that prior control of communications on the Internet, regardless of frontiers, should remain an exception;
- Considers that there is a need to remove barriers to individual access to the Internet, and thus to complement measures already undertaken to set up public access points;
- Expresses its conviction that freedom to establish services provided through the Internet will contribute to guaranteeing the right of users to access pluralistic content from a variety of domestic and foreign sources;

[150] http://en.wikipedia.org/wiki/Convention_on_Cybercrime, Last updated Aug. 8, 2014

[151] http://epic.org/privacy/intl/ccc.html

- Underlines that freedom of communication on the Internet should not prejudice the human dignity, human rights and fundamental freedoms of others, especially minors;
- Welcomes efforts by service providers to cooperate with law enforcement agencies when faced with illegal content on the Internet.

WSIS

The World Summit on Information Technology meeting yielded the following suggestions for the Partnership on Measuring ICT for Development looking forward:

- That it continues, expand, and deepen its work on information society measurement, including by involving national statistical offices at the earliest possible stages of statistical development.
- That it continue raising awareness and building capacity, paying special attention to low income countries.
- That it consider new sources of data and methodologies.
- That it set up an Expert Group on WSIS Targets.

There was strong consensus that the WSIS process and monitoring of the information society should continue after 2015, at the same time deepening the nature of such monitoring. International cooperation as well as national coordination should continue and build on the multi-stakeholder model.[152]

The Declaration of Internet Freedom constitutes a vibrant defence of online freedoms[153]. Its preamble states that a free and open Internet can bring about a better world[154]. It further aims to get millions of Internet users to sign on to this Declaration[155]. The Declaration supports the establishment of five basic principles for Internet policy:

- Non-censorship of the internet.
- Universal access to fast and affordable networks.

[152] *WSIS+10 High-Level Event 2014- Outcome Document: Forum Track* , http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/OutcomeDocument2014.pdf (last updated 6-11-2014)

[153] http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom, last updated Aug. 8, 2014

[154] http://www.internetdeclaration.org/ last updated Aug. 8, 2014.

[155] Declaration of Internet Freedom, http://www.savetheinternet.com/internet-declaration

- Freedoms to connect, communicate, create and innovate over the Internet.
- Protection for new technologies and innovators from abuse by users.
- Privacy rights and the ability of Internet users to protect their privacy through controlled disclosure of information about them.[156]

Framework Gaps

What is distinctly missing however is an international regime on Internet freedom accepted by all stakeholders. Further, Internet freedom as a phenomenon raises various legal, policy and regulatory issues, some of which are discussed below.

Today, many jurisdictions provide fundamental rights/national legislations guaranteeing freedom of speech and expression in the actual world. These same rights have also been interpreted or applied to Internet freedom of speech and expression. However, the Snowden revelations have highlighted unauthorised intrusions into freedom of speech and expression on the Internet. Unbeknown to the relevant users, their communications in the form of audio, video, images or text are being surveilled by various sources. In effect, the Internet and its various facilities and platforms are becoming vectors for enabling a surveillance-based society. From this it is clear that there are two kinds of people in the world: those who know and those who do not know they are being or have been surveilled.

Increased surveillance and online monitoring is becoming the norm and is having a direct impact on freedom of speech and expression on the Internet. In short, while the Internet is not exactly the 'Wild West', it is also clearly apparent from emerging evidence that freedom of speech in cyberspace is not an absolute freedom.

Norms of civilised behaviour apply equally to cyberspace. This means that Internet content aimed at causing inconvenience, ill-will, hatred, enmity, or that targets a particular person or group of persons should be prohibited by national legislation.

However, the anonymity cloak afforded by the Internet can give ill-intentioned or abusive users a sense of complacency to say and do whatever they want with immunity.

Nonetheless, against this backdrop jurisprudence is emerging in regimes around the world whereby the courts are beginning to strip off this veil of anonymity by directing service providers to disclose the real identity of the persons behind illegal activities. As

[156] http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom, last updated Aug. 8, 2014

already stated, however, the fact remains that there is no international standard defining what constitutes freedom of speech and expression on the Internet.

The 1948 Universal Declaration of Human Rights does provide certain basic principles that could be read as being fully compatible with the concept of Internet freedom.

Emerging challenges

Social media networks have brought forward new kinds of online discourse indicative of peoples' mind-sets. However, laws and legislations across the world have not moved swiftly enough to address the emerging challenges inherent in social media.

Smart phones and other communication devices have heralded the emergence of the mobile web. The combination of mobile phones and the Internet enables hitherto unknown manifestations of online free speech. The problem arises when different countries have different ways of dealing with inappropriate online content, and that the ambit of online free speech differs from jurisdiction to jurisdiction. Despite these differences, there is universal agreement in one area e emergence of the mobile web. The combination of mobile phones and the Internet enables hitherto unknown manifestations of online free speech.

Another issue discussed earlier relates to the ability to communicate freely and anonymously on the Internet. As already stated, some people believe that Internet anonymity allows them to say whatever they want online, without needing to worry about its potential impact on others[157]. Often, the victim of alleged online defamation files a lawsuit against a "John Doe" defendant.

Different countries have different defamation laws dealing with various kinds of defamatory speech or content. These laws are equally applicable in cyberspace. In this regard, there is increasingly broad clarity in emerging jurisprudence that no one has the right to defame another person, or to try and damage the reputation of others.

The provisions of national laws vary from country to country in this respect. Some countries only restrict access to the Internet when they consider that it is justified to protect moral values, personal legal rights, national defence, or State security. Others have formally recognised that the right to freedom of expression extends to cyberspace, or are considering such a step.

[157] Eric Sinrod, *"Freedom of anonymous online speech has potential limits"* http://www.lexology.com/library/detail.aspx?g=7a8eb382-b007-49c6-8ca1-4a9197062d9d, last updated Aug. 8, 2014

We are all living in a transitional era of human history in which Internet freedom is threatened not only by State entities, but also by private players who are actually managing and controlling data on the Internet.

Other Challenges Impacting Internet Freedom

Internet jurisdiction is an important issue complicated by the fact that a person’s freedom of expression on the Internet may be curtailed within the territorial boundaries of a nation, whereas you may be physically located within the jurisdiction of another country. Further, the fact that you are invariably being targeted by cyber criminals can also be a contributing factor to non-effective enjoyment of Internet freedoms. Thus, cybercrime has becomes an important legal, policy and regulatory issue that can potentially impact the Internet freedom of users everywhere.

Another issue impacting Internet freedom relates to cyber security. One can only enjoy one’s legal freedom on the Internet provided it is safe, secure and reliable. However, breaches of cyber security have once again brought to the fore the distinct challenges faced in regard to the protection and preservation of cyber resources and infrastructure.

Internet freedoms will have to be seen from a different perspective altogether given the global importance and vulnerabilities of this cyber medium. With the upsurge in cyber attacks targeting computer systems and networks in various countries, Internet freedom will have to be balanced with the need to protect and preserve cyber security.

Countries the world over are still not unanimous about how to deal with the issue of intermediary liability. Some countries like the US tend not to attribute such liability to service providers. Others sometimes mandate intermediaries to exercise due diligence in cases where they want to avoid liability for potential third party liability for online data, while discharging their obligations with respect to certain basic provisions of national law.

The emergence of the ‘dark net’ is another formidable challenge to Internet freedom. Cyber criminals do not hesitate to engage in this domain to carry out their malicious plans and activities aimed at prejudicially impacting peoples’ enjoyment of Internet freedoms.

Yet another major challenge to confidence in the use of cyberspace and Internet freedoms is the growing phenomenon of cyber warfare, which is now an open secret. The advent of cyber terrorism further empirically impacts the full enjoyment of Internet freedoms.

Clearly, there is a need for international understanding and common denominator principles in the context of Internet freedom. Much work has been accomplished in respect of the important legal and policy issues impacting Internet freedom referred to above. It is in this context that organisations like the World Federation of Scientists and the International Telecommunication Union can continue to play an important role in helping to facilitate evolving consensus on the way forward.

Big Data

At this juncture, the impact of big data on Internet freedom should not be ignored because, ultimately, this freedom has to be viewed in the context of electronic data and information. Today, the Internet is a gigantic network of networks, a huge data dragon with infinite memory. One must therefore also consider that Internet freedom in all its forms has a direct connection, association and relationship with big data.

Big data is the big reality of our times. With so much data being generated by different computer systems and networks, it is only natural that companies would want to engage in big data analytics. Big data is defined in various ways by different stakeholders, and is also an important legal, policy and regulatory issue.

Definition of Big Data

Wikipedia defines big data as follows: "[…] an all-encompassing term for any collection of data so large and complex that it becomes difficult to process using on-hand data management tools or traditional data processing applications. However, big data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process within a tolerable elapsed time".[158] **The Oxford Dictionary** defines big data as: Data sets that are too large and complex to manipulate or interrogate with standard methods or tools[159]. **The White House report on big data** issued on 1 May 2014 echoes the now widely accepted definition that big data "[…] is so large in volume, so diverse in variety or moving with such velocity, that traditional modes of data capture are insufficient".[160] **Tech America Foundation** states: "Big Data is a term that describes large volumes of high velocity, complex and

[158] http://en.wikipedia.org/wiki/Big_data

[159] http://www.oxforddictionaries.com/definition/english/big-data

[160] http://www.lexology.com/library/detail.aspx?g=e7161021-7570-476c-bf8a-b4637d10a355

variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information."[161]

The various features of big data include:

- That it should be elastic in nature[162].
- Many big data systems take in uncurated data, meaning that there are always data points that are extreme outliers, introducing 'hotspots' in the system.
- Big data can rapidly obtain requested compute cycles by leveraging a cloud-based Infrastructure as a service[163].
- The quantity of data generated is very important in this context. It is the size of the data which determines its value and potential under consideration, and whether or not it can actually be considered as big data.
- Variety is about managing the complexity of multiple data types, including structured, semi-structured and unstructured data.
- The speed at which data is created, processed and analysed continues to accelerate. Contributing to higher velocity is the real-time nature of data creation, as is the need to incorporate streaming data into business processes and decision making.
- Data uncertainty: Veracity refers to the level of reliability associated with certain types of data[164].

There are multiple legal, policy and regulatory concerns pertaining to big data. First and foremost, it should be noted that there is no international framework – or international treaties – dealing with big data. As such, big data is one subject that continues to be regulated by national legislations. It is the case that most countries do not have dedicated legislations or legal provisions in this regard. For the purpose of

[161] TechAmerica Foundation, Demystifying Big Data: A Practical Guide to Transforming the Business of Government 2012, https://www-304.ibm.com/industries/publicsector/fileserve?contentid=239170, last updated Aug.4, 2014.

[162] http://hadoopblog.blogspot.in/2012/02/salient-features-for-bigdata-benchmark.html

[163] http://www.dummies.com/how-to/content/characteristics-of-big-data-analysis.html

[164] IBM, Analytics: The real-world use of big data- How innovative enterprises extract value from uncertain data, http://www.ibm.com/smarterplanet/global/files/se__sv_se__intelligence__Analytics_-_The_real-world_use_of_big_data.pdf last updated Aug. 8, 2014.

policy and regulatory frameworks, however, it is imperative to consider the important parameters referred to below.

Data protection is one of the biggest big data challenges. Different national jurisdictions have different regulatory requirements for data protection. The European Union has data protection directives, while countries in other regions have incorporated various data protection provisions into their respective national legislations. Methods of data collection, protection and preservation are important considerations. Big data protection requires a distinct revisit since data protection legislation has always been framed with respect to relatively small data quantities generated by individuals, which are miniscule compared to big data volumes.

Big data protection faces immense challenges, both for processors and regulators. Its massive volume and its referencing and diverse sourcing architecture call for a distinct safe and secure legal framework that helps to protect both data users and suppliers.

Data minimisation also raises privacy and data protection issues. Of particular relevance is the need to develop appropriate international best practices for the collection, retention and destruction of data, including personal data in identifiable form.

National legislations differ on the issue of individual consent for the collection, use or disclosure of data versus individual data control. As already mentioned, there is no international legal arrangement covering big data on this and other issues related to cyberspace.

Another legal issue pertains to data anonymity and data masking for the persons placing information on the Internet. An important question which has not been appropriately addressed concerns the basic principles that should be applicable in the context of big data collection, processing, retention and dissemination. Given the fact that big data today is invariably on the cloud, its protection and preservation constitute further legal, policy and regulatory challenges.

Data privacy is an important big data issue due to the huge data volumes consumed, and also because every data provider has an intrinsic right to the protection and preservation of h/her data. Hence, the responsibility for ensuring adequate protection of this data lies squarely with the network service.

Big data jurisdiction is also an important legal, policy and regulatory issue because such data is invariably located on the cloud and on various other servers located in different parts of the world. In cases where big data privacy is breached, the concerned person should take legal action against the relevant service providers. The big challenge will be to identify the physical location of the said data since determining the location of the server where the breach occurred would have ramifications in terms of local privacy encroachment laws.

Cybercrime in relation to big data is also a significant legal challenge because the entire Internet economy is based on this data, and unauthorised privacy encroachments of big data can significantly assist cyber criminals, which is why they are likely to target this domain ever more frequently.

In October 2013, Adobe confirmed that cyber criminals had illegally gained access to its network, obtaining more than 2.9 million user names, encrypted credit and debit card numbers, card expiration dates, login IDs, and passwords. Adobe's source code for several products, including Acrobat and ColdFusion, was also accessed[165].

The European Network and Information Security Agency (ENISA), an EU advisory body, stated in January 2013: "Exploitation of big data will affect data privacy. At the same time, exploitation of big data through adversaries might open doors to [a] new type of attack vectors".[166] ENISA added that big data is the aggregation of information generated "[…] as a consequence of the proliferation of social technologies, cloud computing, mobile computing and the Internet use in general," and had become an emerging security issue.

Privacy

Big data analytics could have a direct impact on the violation of personal privacy. In May 2014, the White House released its long-awaited report on big data: "Big Data: Seizing Opportunities, Preserving Values". The report was requested by President Barack Obama and addresses the ways in which technological advances are rapidly evolving to allow for the collection, storage, analysis and use of vast amounts of big data both by governments and the private sector. It highlights the potential threats to individual privacy and equality that may derive from big data, now and in the future., and also advocates legal, policy and regulatory initiatives to protect citizens in the US and globally from potential abuses.[167]

[165] http://blogs.mcafee.com/consumer/consumer-threat-notices/malicious-acrobatics-adobe-the-latest-target-in-string-of-cyber-attacks

[166] http://www.out-law.com/en/articles/2013/january/cloud-mobile-social-and-big-data-technology-innovations-increasing-threat-of-cyber-attacks-says-eu-body/

[167] Kenneth R. Florin , Ieuan Jolly et. al "White House "big data" report highlights benefits and potential for abuses from big data" http://www.lexology.com/library/detail.aspx?g=a036aed0-cffb-4ae1-a518-44b92201effb, last updated Aug 4, 2014

Big data and data privacy are thus assuming growing importance in the legal world. There are often going to be disputes over who owns big data content, even more so when third parties are involved in developing systems designed to generate it. Data protection, including sensitive personal information using cryptography and granular access control, is another major concern.

Big data retrieval and access also have an intrinsic connection with privacy, and are predominant legal issues in the context of preserving mined data and data analytics. Of prime concern is the maintenance of the authenticity, integrity and veracity of accessed and retrieved big data.

Further, the use of cryptographically-enforced data-centric security raises its own legal issues. In addition, granular access control entails various other complicated legal and policy privacy issues. Furthermore, there is a need to safeguard privacy during the dissemination of information.

Another big data concern is that once it is collected it can be very difficult to preserve its anonymity. While promising research projects are underway to obscure personally identifiable information within large data sets, far more advanced efforts are presently being undertaken to re-identify seemingly "anonymous" data. Collective investment in the capability to fuse data is many times greater than that devoted to privacy-enhancement technologies[168]. A prime concern is to ensure the authenticity, integrity and veracity of big data earmarked to be accessed and retrieved.

Other legal issues relate to securing big data infrastructure in terms of having an appropriate legal framework for protecting computations in distributed programming structures. In this connection, appropriate best practices for enforcing and maintaining security for non-relational data stores should be developed. Yet another major legal issue relates to data management. In this regard, appropriate enabling legal frameworks are needed to secure data storage and transactional logs, as well as granular audits.

Intellectual property rights with regard to big data constitute a further major legal issue. Who has the intellectual property rights to big data? What are the intellectual property rights related to the collection, storage, processing or sharing of big data? Often there are concerns that the new big data search and analysis tools could result

[168] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values,* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf, last updated Aug 4, 2014

in infringement of data copyright. Determining the liability of the relevant contracting parties for inaccurate or incomplete information, or for when contractual agreements are not honoured are other concerns.

It is also possible that technology opens up the possibility for unauthorized access to information on business competitors, which gives rise to various competition law issues. The fact big data profitability depends on such trade secrets and sensitive personal data in itself has an impact on meaningful privacy and security – and erodes confidence in the use of cyber platforms and technologies.

It has been argued that big data collection and processing have an influence on peoples' individual and collective identities, which risks eroding the quality of democracy.

An additional concern relates to the fact that many big data censors are predominantly powerful intermediaries, increasing the risk of them being misused and abused to violate individual rights and liberties of individuals.

In short, there is a need to come up with an appropriate enabling legal framework to ensure that big data does not in any way prejudicially impact the enjoyment of citizens' rights – or indeed the fulfilment of their civic obligations and duties.

Role of World Federation of Scientists and ITU

Given the absence of international parameters pertaining to legal and policy frameworks for big data, it is imperative that organisations like the World Federation of Scientists and the International Telecommunications Union pursue efforts to facilitate their development.

Conclusion

In conclusion, it can be stated that both Internet freedoms and big data are very fascinating and evolving concepts that play an increasingly significant role in our daily lives. It is therefore of capital importance to develop and implement appropriate international legal, policy and regulatory frameworks to preserve Internet freedoms. At stake is the very future of these digital age structures that serve us so well and upon which we have grown so dependent in so many ways.

The important task ahead is to formulate and implement these international policy and regulatory frameworks based on universally accepted principles.

These frameworks will necessarily develop over time. Numerous jurisprudence initiatives are currently underway in regard to Internet freedoms and big data.

However, it is imperative that efforts are made towards ensuring the development of effective policy and regulatory frameworks at an international level.

The World Federation of Scientists' Permanent Monitoring Panel on Information Security can play an extremely important role in this regard, not only in a monitoring capacity but also in contributing to the development of such international frameworks. Together with the International Telecommunications Union, it is hoped that the World Federation and other relevant organisations are able to make a significant contribution towards this goal, commensurate with their expertise and experience in these domains. It would certainly be of considerable value to all stakeholders if these organisations were able to help develop universally accepted common denominator principles that aim to ensure an appropriate cyberspace environment.

As already mentioned, at stake is the ability of all users to continue enjoying the benefits of Internet freedoms by overcoming cybersecurity and other challenges that risk eroding confidence in this expanding and ever more essential universe.

One hopes that relevant jurisprudence will develop apace with the growing number of Internet users and the accelerating speed of cyber-tech progress. Only by constantly following relevant jurisprudence developments and by contributing to progress in this respect will it be possible for the world at large, and specifically for key players, to chart the way ahead.

The process of developing relevant legal, policy and regulatory frameworks for big data and Internet freedom will evolve over time. Extending respect for the fundamental rights to cyberspace will be an important prerequisite for success in this regard.

3.3 A Global Perspective of State Surveillance in Cyberspace

By Howard Schmidt

Introduction

In order to properly understand and render a considered opinion on the topic of surveillance in cyberspace, it is important to first understand that our frame of reference is largely based on a world where the rules of engagement (written or otherwise) have evolved over time, notably during the period that far precedes the advent of what we call cyberspace.

For every person who considers that surveillance is justified, there is always someone with a contrary view – and a vast number of stakeholders who live in a grey area with respect to the subject. It is through exploration of empirical information and application of reason from a global perspective that we can eventually come up with a balanced set of guidelines that all stakeholders can consider when determining if State surveillance is both appropriate and justified.

Data Collection

The growth in technology has created an environment where vast amounts of data are created, transmitted, and collected for various purposes. Everything in cyberspace that is produced is done so from data, and capturing this data is essential, as is the collection of the captured data. Examples of essential data that must be captured and collected are financial transactions. Consider, if you will, the modern pay check. Many of us receive our compensation in the form of electronic fund transfers that are deposited into our accounts, and many of us collect and archive this electronic data in the form of a savings account. This archived data can be moved to another collection point in the form of a transaction (such as in a grocery store) where goods are exchanged for the data that represents a financial instrument.

Another example of data that is collected in a related manner is a mobile phone call between two parties, where the mobile phone company keeps track of where the call was placed, when it was placed, and the duration of the call. This is intended for billing purposes, as the phone company explains to us as consumers. Websites collect data from users of the website and services for various purposes, some of which include setting and maintaining user preferences and archiving pieces of information the user has created (such as a social media website).

As citizens in cyberspace, we all understand and accept that there are circumstances where collecting data is not only reasonable and acceptable, but in many cases desirable. What drives acceptance of data collection by stakeholders is a clear understanding of what data is collected, and for what intended purpose. In such cases, we choose to accept the terms that accompany the collection of data before engaging in the associated activity, or choose not to engage in the activity if we feel that the data collection and usage policies are too onerous.

In essence, as stakeholders we all agree to a contract with those who have access to our data which articulates how the data can be collected and used, who can be the data custodian (e.g. the cell phone company), and to what extent the latter can transfer custody, and to whom. Data custodians have an enormous amount of power with respect to the data, but this power does not grant them authority to do with the data as they choose. Ultimately, once a custodian chooses to use the data outside of the agreement in place with the person or organisation that the data is tied to, h/she must enter into a new agreement that allows this expanded use. Failure to do so can be reasonably construed as an abuse of authority, or violation of trust.

Judicial Process vs. Intelligence Gathering

It is for the aforementioned reasons that we have processes in place today that allow for the expanded use of data beyond the expectations of the stakeholders concerned. In cases where there may be a reasonable suspicion that someone is involved in criminal activity, legal and judicial processes exist that allow for the monitoring of and access to collected data that can be used to serve as evidence of wrongdoing. The rules and procedures associated with this type of surveillance vary globally, yet the general populace typically has access to the rules of engagement.

Where things become a bit murky is in situations where the surveillance is through government intelligences agencies. On a global level, intelligence agencies covertly monitor and gather data, and use the information for various purposes. Ostensibly, most agencies will claim that the gathered intelligence is for national security reasons (e.g., as in the case of the recent NSA disclosures), or the greater good. Others may simply claim that their sovereign authority allows them to do so, and that they essentially do not need to explain why they engage in intelligence gathering activities. This becomes particularly challenging in a global economy where two or more nations differ in their positions on such data gathering activities. In such instances, cyber citizens may believe that they are afforded a level of confidentiality in line with the rules of their government, but transmit information in cyberspace, where the pathways data take from origin to final destination may cross national boundaries. Once the data lands in a location where the rules are different, it is subject to those rules. Since intelligence gathering is a closed process not typically subject to the transparency expected in law enforcement and judicial procedures, it becomes exceedingly difficult to determine when a line has been crossed.

Methods and Rules for Intelligence Gathering

If intelligence gathering is permitted outside a legal or judicial process (and in many cases it is), then it is important to consider the use of malware and covertly placed applications by the intelligence gathering communities. In many sovereign States, creating malware and applications intended to infiltrate computer systems through various propagation methods is highly illegal in and of itself. Any activity the malware engages in once it has propagated is also considered criminal activity on the part of the malware creator, as is any user or organisation knowingly propagating and using the malware to engage in such activities. The legal and judicial processes established globally currently govern this, and the punishments can be quite severe for breaking the law in this regard.

Once again, when considering how State-sponsored intelligence gathering communities operate, the rules for engaging in activities involving the creation and propagation of malware and covertly cloaked applications, and for gathering the data associated with the use of such “tools”, are very murky. Depending on the specific sovereign State being considered, it may be deemed acceptable for a government intelligence organisation to engage in such activities for various reasons – perhaps most commonly on national security grounds. It is, however, important to note that once malware is deployed it can (and often does) propagate far beyond the intended boundaries, and negatively impact systems that would be considered clearly out of bounds to the intelligence-gathering agency by all accounts. An example of this would be critical systems, such as hospital networks, power grids, and safety systems used to control hazardous processes (such as chemical production). Additionally, financial systems, food production systems, and manufacturing systems can be negatively impacted, which can create an avalanche of social unrest and panic.

Levelling the Cyber Weapons Playing Field

One can consider the use of malware as described here the equivalent of launching a cyber weapon, with the understanding that the weapon can have an effect on much more than the intended target. Moreover, the ability to create and deploy cyber weapons is not limited by any of the economic and natural resource constraints typically encountered in traditional physical conflicts. The existence of metals, chemical facilities, or high tech tools has little effect on the capabilities of malware creators. A computer and network connection, or external media storage and transportation (e.g. a USB memory stick) is more than adequate, coupled with the knowledge of how to create the malware.

Once malware has been created and propagated, it can then be weaponised and used by any person or organisation that can identify and isolate it. This means that the originating organisation can have the cyber weapon turned against them, possibly via a mutated version that enhances the functionality of the original malware package. In such cases, the organisation that introduced the malware initially acts as a global supplier of the cyber weapon. This effectively means that, beyond the advantages gained by the first strike, the playing field becomes levelled for all parties soon after the initial launch, and can lead to a highly destructive environment where no person or organisation can find a safe harbour. Moreover, once cyber weapons are deployed, they essentially exist forever, as there is no stockpile to eliminate.

The Way Forward

It stands to reason that regardless of the intentions of those who engage in surreptitious State-sponsored surveillance, there are consequential challenges that emerge with potentially uncontrollable and unforeseeable negative repercussions. This can create ripple effects that can potentially destabilise global relations and economic conditions. While the Internet can serve as an effective way to engage in surveillance for what some may view as good intentions, it is important to understand that the Internet has grown into an integral and necessary part of the world economy, allowing individuals, organisations, and nations of all sizes to participate as equals. It also allows for the free exchange of ideas instantaneously, and for collaboration at every level of the economic food chain.

It is therefore important for the global business community at every level to exert pressure on governments everywhere to pass relevant laws. Such laws should serve to prevent the potential disruption of the economic and social benefits derived from the internet. They should also allow for continual growth in the numbers of individuals, organisations and nations that can participate in a collaborative economy fuelled by a stable Internet where everyone can remain confident in knowing that government interests are not put before those of the people they serve.

3.4 The Extent of State Surveillance in Cyberspace: A European Union Perspective

By Henning Wegener

The inherent and growing tension between the freedom and integrity of the Internet (and digital communication generally) and, on the other hand, the increasingly urgent requirements of public order and collective security concerns, is amply reflected in many parts of this publication, especially in Prof. Al Achkar’s essay on Internet freedoms and civil liberties on the Net.

With the current visibility of massive intrusions into digital devices and networks and the Big Data scare, this tension is now more than ever at the forefront of widespread popular anxiety in Europe. The extraordinary growth of technical possibilities for data collection and handling, propelling mankind into a new era of lost privacy, has raised fears that principles of national and international law and personal and collective assets are in grave peril. The increasing encroachments on the underlying human rights have rightly become a global issue, and the definition of rules and limits to this seemingly unstoppable wave cry out for remedial action on a global level.

An important beginning in setting the necessary policies has been made with UN General Assembly Resolution A/RES/68/167, adopted without a vote on 18 December 2013, "The right to privacy in the digital age", expressing the willingness of the international community to act against the mass surveillance, interception and collection of personal data. In pursuance of operative paragraph 5 of that Resolution, the UN High Commissioner for Human Rights has, in June of 2014 forwarded a Report (A/HRC/27/37) which was debated at the Human Rights Council in a panel discussion in September at its 27th Session, and is expected to be taken up by the UNGA at its current 69th Session "with views and recommendations" contained therein to be considered by Member States. The Report states unequivocally the human rights requirements for state surveillance measures: they must be necessary and proportionate, transparent, and respectful of the rights to privacy of individuals abroad. The Rapporteur makes it clear that he does not feel that these requirements are currently met.

Awaiting concrete outcomes from these global proceedings, and in spite of universal needs and approaches, there are telling regional differences in how nations and populations react to the revelations and realities of intrusions into digital privacy, national sovereignty and protected information domains (in a vast public debate triggered by the Snowden case).

In some parts of the world, there is more resignation than revolt, or even indifference; in many of the biggest countries, public voices of rejection are muted by the prevailing political systems; in the US, there is a substantially higher understanding of alleged or real public security needs, supported by a more lenient legal system. In Europe, and mainly in the European Union, on the other hand, the revelations and the sheer dimensions of the illegal data thefts have caused a storm of dismay and rejection. A political ground swell has developed which it would be lightheaded to underestimate, not least in its transatlantic dimensions of collective loss of confidence – cyber confidence as it were. The perennial close relationship of the European democracies with the US, underpinned by a strong emotional attachment, is no doubt affected.

This collective sentiment in Europe reflects its fervent desire for freedom and privacy, assuredly largely amplified by its recent history marked by dictatorships and their negation of personal privacy (still vivid in memories), but also by its highly developed state of data protection and civil liberties, and the very nature of the European Union as a legal entity. The fear of an all-powerful Big Brother, a Leviathan unrestrained by any law, is much more present in Europe than elsewhere, even though it would be wrong to underestimate the collective dismay of Americans too in reaction to massive government surveillance. The controversy is likely to play a central role in the next Presidential elections.

Yet, precisely if we seek to define global criteria for maintaining cyber confidence in an era that enables limitless technical means of intrusion, a look at the EU scene and its legal environment might be recommendable, as it may help to establish an important pillar of a universal regulatory framework.

One reason for this is that the EU constitutes a law-based community of 28 highly industrialised nations which play a major role in the world digital economy, and where digital technologies have become more than elsewhere the paradigm of the economy and society; still today, the EU is the world's biggest economic block. This makes EU countries proportionally more threatened by cyber attacks than many others; McAfee has determined that Germany, for instance, with a damage rate from cyber attacks situated at 1,65% of its GNP, holds the record among industrialised countries At a time when cybercrime consortia are a main driver of damage to highly net-dependent, open economies, and where foreign spy services are having a feast, cyber criminality has become a grim reality in Europe. It has motivated the European Union to develop a highly advanced collective and uniform cybersecurity system.

The EU is at the same time a grouping of 28 independent countries, and an organisation with common institutions and norm-setting faculties. The majority of legislative acts result from joint action of the European Council – on initiatives by the EU Commission – and the European Parliament. Resolutions and Decisions are immediately binding for all member States in all their parts, in line with Directives on implementation of the agreed objectives. These Resolutions and Decisions have to be transposed into the national laws of member States – a unique feature of the international system. The common institutional basis of European legislation does not only produce immediate legal effect within the member States, but also impacts on the world beyond. The EU can thus form an example that many may find worth emulating, as an institutional laboratory where a big group of nations try out what can also be implemented in the community of nations at large. EU legislation is a forceful instrument of internal coordination and harmonization, but also a pathway to international regulation.

Both cybersecurity and policies for guaranteeing the protection of personal data are within the competence of the European organs. As regards cybersecurity, the European Commission has been working on a regulatory framework for its member States for more than a decade. A sequence of important documents, in part analytical and in part prescriptive, have produced a comprehensive body of law, obligatory for EU member States, which, both in scope and detail, has no equal in the digital world of nations, except in the US. In addition, in 2004, the 28 member States created the

European Agency for Network and Information Security (ENISA) as a joint think tank, a coordinator of important joint EU activities, and a stimulant for further regulatory action. Mention should also be made of the European Cybercrime Centre, attached to EUROPOL, and a Europe-wide CERT as the central point of contact and action in case of cyber attacks. There is no space her to depict the whole range of EU cybersecurity activities, in its legal and institutional dimension, but an overview can easily be obtained by consulting the ENISA web page, and other available analyses[169]. The EU is firmly set on its Digital Agenda, and on optimizing cybersecurity. The two comprehensive recent documents, incorporating earlier norms that merit study, are the 2013 Cybersecurity Strategy of the European Union[170] and the Draft Directive for Network and Information System Security (NIS)[171]. Both, but specifically the NIS Directive, stipulate comprehensive requirements, standards and obligations for the private sector, CERTS, operators of critical infrastructures, networks, and information systems.

The point of interest in our context is that the EU constitutes a territory of harmonised cyber law. 23 of the 28 countries have incorporated the Budapest Convention on Cybercrime into national law (the remainder will no doubt do so shortly) and all have incorporated the (similar) Directive of 2002[172]. Cybercrimes, and any intrusion into digital devices and networks are thus equally sanctioned in all EU countries, and law enforcement can take its course anywhere in the Union.

Another important aspect of EU digital policy is data protection. The protection of personal information and the private sphere of individuals have become relevant only with the development of digital data storage. The applicable EU laws are far-reaching. The current legal basis is still EU Directive 95/46EG, which spells out minimum protection standards, that all EU members have since incorporated into their respective national legislations. The Directive applies to the personal data of individuals. Use of the data is legitimate if the person concerned has expressed

[169] www.enisa.europa.eu. See also Henning Wegener, *La ciberseguridad en la Unión Europea,*www.iees.es/Galerias/fichero/docs_opinion/DIEEE077bis-2014_CiberseguridadProteccionInformación_H.Wegener.pdf. A German version of the paper is available at www.unibw.de/infosecur.

[170] JOIN (2013)1 final

[171] COM (2013)48 final

[172] COM (2002)173 final

consent, or if other narrowly defined circumstances are present. The restrictions also to some extent apply to data users from outside the Union[173].

In 2010, the EU Commission launched a more ambitious legislative project to adapt the extant data protection to changed circumstances[174]. The draft Regulation – General Data Protection Regulation (GDPR) - attempts to capture the needs of an advanced information society characterised by vastly increased data flows, cloud storage, new social networks, and the exponential increase in connectivity. As a Regulation the new text, once adopted, would be immediately obligatory in all member States and create a uniform body of EU law, including a detailed single set of rules for all 28 members. The Regulation is more stringent and detailed than the 1995 Directive and provides for heavy fines in case of violation. The draft text passed the European Parliament in March 2014 and is presently being discussed by governments with a view to a decision in the European Council. It is expected to be final in the next few months, and will then enter into force in 2016. Yet, it already has anticipatory effects, as it shows that the EU is heading towards a very tight data regime.

After this brief overview of existing and impending European law as a coherent legal fabric, we can now return to the problem of surveillance in cyberspace. Any intrusion into digital data carriers – computers, telephones, networks, other digital devices – and the copying, theft, change or transfer of stored data – is a cyber offence, if no specific justification exists. If there is intrusion into digital devices and nets, and if personal data are concerned, it also violates data protection laws. Cyber criminality and tampering with personal data thus are closely intertwined, and both bodies of legal prescription need to be invoked. Internet Freedom is at stake in both categories of cyber delinquency.

Industrial or political espionage on the Internet (or the cloud, or other storage areas), i.e. the theft of, or tampering with political facts or commercial data not including personal data, is not sanctioned by International Law. It is however subject to sanctions in countries with appropriate legal coverage under normal penal and civil law, no matter whether the perpetrator is an individual, enterprise, institution or foreign government. In EU countries, the Budapest Convention and/or internal

[173] For most of the EU member States, two other international instruments are also relevant, the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, and the European Data Protection Convention of the Council of Europe which is binding in the 46 signatory States.

[174] COM(2012)11 final

legislation provide the necessary handle. In penal law, that holds even if the attack has come from outside national frontiers, if the offence has effects or causes damage inside them. Under the Convention a State member is required to punish cybercrimes committed in its territory, also if the perpetrator is not a resident there[175].The ubiquity of the effects of cyber offences thus moves cybercrime law towards becoming a chapter of World Penal Law, although it may not yet be universally adopted or applied, especially in cases where the originating State is uncooperative, or is itself the perpetrator. If the surveillance and capture of data includes personal data, the prohibitions and penalties of the data protection laws apply in addition.

The simple truth is thus that the current massive intrusion into digital space by governments, domestic or foreign, and private originators under EU law, and wherever comparable legislation exists, constitutes a severe breach of law, unless the intrusion is justified by public security and public order concerns and has been authorised by national law and the required legal procedures – thus making it legal. To be precise: notwithstanding widespread practices by governments, cyber attacks abroad can in no way be justified by national convictions, perceived security requirements and the available legal procedures of a foreign government, until it also has the express consent of the government where the intrusion occurs, or exerts effects. In the EU, joint action by member governments is frequent, and thus legal. These principles cover the large-scale surveillance of international Internet connections, node points, wireless connections, etc. This is rendered more poignant by the reported extent of limitless data collection – a true collection fury –by foreign security services. Such data collection benefits from unprecedented technical prowess and means, but visibly goes beyond a pragmatic assessment of risks and an acceptable security rational, often with no concern for friendly governments, data protection, human rights, and damage caused[176].

There are, of course, several caveats to add to this reading of the legal situation, caveats whose validity goes beyond the EU. In the first place, cyber attacks, benefiting from the basic anonymity of the Net, are hard to detect. Lack of attributability and tracking and tracing difficulties in many cases make law enforcement futile or at least complex. If a data attack is launched from abroad, the added difficulty if the State of origin is uncooperative is to get hold of the perpetrator. That, of course, should not prevent us from setting the legal record straight. Secondly, the activities of foreign governments mostly operate under the cloak of sovereignty and individual diplomatic

[175] See para. 233 of the Explanatory Report to the Budapest Convention on Cybercrime

[176] The Report by the UN Human Rights Commissioner cited above makes this point forcefully.

immunity of the perpetrators; many surveillance activities are, however, performed by private contractors where this logic would not hold. However, the inability to prosecute – in principle with recourse only to diplomatic procedures – does not change the underlying legal situation. In countries where the public prosecutor does have to act ex officio in case of suspicion of criminal wrongdoing, as in most EU countries, there would be an obligation to initiate criminal proceedings even though an accused may claim sovereign inviolability. In Germany, criminal proceedings against "unknown" are presently underway to prosecute illegal eavesdropping on the mobile telephone of the head of government. In the interest of legal hygiene it would be desirable that such proceedings become more frequent, or even the rule.

Thirdly, it would probably be wise to formulate – preferably in an international setting – doctrine for digital surveillance by State security services, national or foreign, without prior authorization in case of "clear and present danger", an imminent major terrorist threat, if criminals are caught red-handed, an impending major crime or attack against critical infrastructures, and the like. Post-fact authorization is always possible.

The current sense of revolt in most European countries against the massive intrusion and spy activities by US agencies – but also by other countries – appears somewhat exaggerated and artificially engrossed; and before attempting to look for reasonable criteria to separate the necessary from the strictly unacceptable, it might be useful to inject a sense of realism into the debate, and to de-dramatise the situation[177].

In the first place, it is unavoidable not to take note of the unprecedented technical progress that enables massive intrusion into digital devices, large-scale data collection, and processing with powerful search tools. To make use of these technologies with the purpose of improving national security policy cannot be condemned as a matter of principle. These technologies cannot be disinvented, and they are here to stay. New technologies are used once they are available, and the wheel cannot be turned back.

Second, the intelligence services of EU countries have equally used these techniques, often in close conspirational cooperation with their US counterparts. All or most of them employ these technologies in their foreign operations, and even at home. That holds true in particular for the United Kingdom where US data and practices from the PRISM programme are used without the required "warrants" or judicial control. They

[177] Similar attempts have been undertaken by Nigel Inkster, *The Snowden Revelations: Myths and Misapprehensions,* SURVIVAL, February-March 2014, p. 51; Joachim Krause, *Diskutieren statt moralisieren,* Internationale Politik, January-February 2014, p. 108

are even used there in the absence of concrete criminal suspicion, but also where huge quantities of random data are obtained by eavesdropping social networks, tapping all fibre cables running through UK territory ("Programme TEMPORA"). The resounding indignation in many European quarters about US practices thus has an element of hypocrisy.

Thirdly, the security gains of US practices in the fight against terrorism, organised crime, money laundering, etc. are undisputable, and, given the technological superiority of the US services, examples abound showing that the European allies have been among the prime beneficiaries.

In this sense, one can legitimately discuss the extent of the surveillance measures, but much less the basic justification for them. As regards extent, only a fraction of the data obtained or accessible by the US services are actually used. According to NSA 2013 figures, the quantity of data circulating on the Internet daily amounts to 1,828 petabytes. The NSA can capture only 1, 2% of these, and examine only a small fraction of them. This would be the equivalent of only 0, 0004 % of data traffic on the Net, and only this fraction would be scrutinised[178] by filters. It is important to maintain a sense of dimension.

Finally, as mentioned earlier, there is a healthy debate within the US. The country has never been a monolithic block of opinion, rather a vibrant democracy with built-in learning effects. There is a good possibility that on-going processes in the US to revisit surveillance and data protection policies and practices may finally result in a more congenial transatlantic situation. Already in January 2014, President Obama announced damage-limitation measures[179]. These provide, *inter alia*, for more stringent administrative control of the sometimes freewheeling intelligence operations; data collection only for strictly public security purposes; telecommunication data to be stored primarily with industry, and to be accessed by the intelligence services only on judicial authorization.

The preceding arguments, intended to calibrate the debate, are in no way meant to trivialise excessive and reckless data collection as now practiced. There is no doubt that the transatlantic perspectives on data surveillance and protection, and on the

[178] Data from Joachim Krause, ibid p. 114. Considering the source, NSA, some doubt the veracity of these figures, but even if only indicative, they show that the Agency is not capable of surveilling more than a fraction of the Internet traffic, that it concentrates on security- relevant partial data, and that it remains far away from total data capture.

[179] "Presidential Policy Directive-PPD 28, www.whitehouse.gov.

necessary legal constraints are still far apart, very much for reasons of history, legal tradition and the traumatic experience of 2001 terrorism. There is simply not the same understanding of the balance of security and freedom. And the gap is unlikely to close soon. Despite the legal dubiousness and the basic opprobrium attached to spying and illegal intrusion, these practices are not likely to disappear, even though it is important to be clear about their criminal connotations and penal liabilities. "Spying on allies" is a particularly sensitive issue, affecting companionship, common purpose and even bonds of personal friendship, but is has a long tradition, even in the transatlantic context. But apart from being a breach of etiquette – trust – there is slim chance that allies will rush to conclude formal "no-spy" agreements[180]. Informal understandings would be welcome.

Great quantities of ink have been consumed to offer solutions for the surveillance quandary, especially as regards the EU-USA relationship. The public debate and government discussions are on, and it would thus be pretentious to offer a sermon with firm and comprehensive recommendations for everyone involved. Instead, this contribution will close with some very modest advice.

As regards the EU, it is important soon to finalise the legal documents designed to complete the cybersecurity components of the EU Digital Agenda, the Directive on Network and Information System Security (NIS), but also the General Regulation on Data Protection (GRDP), as common bases for any future agreements with the US and worldwide.

EU member States must also make sure that their own intelligence services comply strictly with European and national law. It would make no sense to ask more from the US as the EU delivers. EU nations should also conclude among themselves an EU-wide mutual no-spy agreement and consider the gradual establishment of an EU intelligence service with full information sharing among Union members. In the meantime, there should be even better coordination of their security services.

National law enforcement in the EU in cyber and data protection matters must be activated to demonstrate where the law lies in the face of shady intelligence and espionage operations.

As a preceding chapter demonstrates, the best cyber defence reposes on heightened resilience, also as regards staving off illegal data collection and information attacks.

[180] See Leif-Eric Easley, *Spying on Allies.* SURVIVAL, August-September 2014, p. 141, Rodri Jeffreys Jones, *Eine Frage der Etikette,* Internationale Politik, September-Oktober 2014, p. 74

There is much room for strengthening the technical resilience of systems and networks, heightening the self-protection of users (better security awareness, better information economy and back-up practices, encryption, etc.). In other words, before wailing, do your homework.

Restoring cyber confidence in a transatlantic context is a difficult task that can yield results only over time. But the time has come to work on a transparent, joint understanding of how a solid balance between freedom and security requirements can be found, and how foreign government intelligence work and surveillance can be made compatible with the provisions of domestic EU law. It is unavoidable that foreign agents be kept to the standards of the country in which they operate. In this respect, the transatlantic cleavage can perhaps not be bridged soon, but it should be narrowed. The EU clearly cannot deviate from its high data protection standards. Work on a revised Safe Harbour Agreement regulating the prerequisites of transfrontier data transfers and their faultless implementation should be initiated.

After the current spate of data prying – the excessive nature of which is widely recognised – there should be a new spirit of proportionality and measure where the immense technical potential for data capture is used with moderation, consideration for interests affected, including human rights, and respect for the legal tenets of the countries in which searches take place. We need a culture of a more sober assessment of security needs, and of restraint.

In the medium term, the global perspective should prevail. The EU should participate in the search for an international regulatory framework, very much in tune with General Assembly Resolution A/RES/68/167, thus contributing to a sound balance between shared security interests and Internet freedom.

3.5 The Limits to Cyber Freedom: A Search for Criteria

By William A. Barletta

Digital telecommunication technology, especially as exemplified by the Internet, has had disruptive societal effects of a magnitude only matched by the electrification of cities and towns more than a century ago. Like electrification, digital telecommunications depend upon widespread, interconnected networks. But unlike the electrical networks (grids) that are regional in extent, the Internet is worldwide crossing national borders and cultural divides. Like electrification, which does not reach roughly two billion “energy poor”. The Internet has a comparably sized class of "information poor". Like modern electrical grids which enable consumers to transmit and receive energy, Internet users both send and receive information routinely, often in equal measure.

Thus, like the legal and policy analysis of energy networks, the analysis of the utility that powers the information society has generated its own terms of distributive justice and moral imperative. Freedom[181] is just such a term – one that motivates many to think of freedom on the Internet as a fundamental human right as defined in the UN Universal Declaration of Human Rights[182] (UDHR*)*. In particular, Article 19 of the UDHR guarantees the right to freedom of expression:

Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Westby notes[183]: "Although the UDHR is not directly binding on UN member states, portions of it, including Article 19, have acquired legal force as customary international law. The formulation of Article 19, "[…] without interference […] to seek, receive and impart information and ideas […] regardless of frontiers" maps well onto the usual taxonomy of Internet freedom that includes freedom of access. Some would elaborate the phrase "without interference" to imply the rights to privacy, anonymity, data security and even further the right to expunge content that they have put on the net.

[181] Internet freedom has been called a plastic term that is used by the U.S. and its European allies in a fight over the future governance of the Internet. See "World War 3.0," Vanity Fair, May 2012.

[182] UN General Assembly Resolution 217A (III), 10 December 1948, http://www.un.org/en/documents/udhr/.

[183] J.R. Westby, The Role of Science and Technology as Empowerment of Person and State, Proceedings of 44th Session, International Seminars on Planetary Emergencies, 19-24 August 2011, Erice, Sicily.

Under Article 19, *Access* to the Internet can be considered as one figure of merit for judging Internet freedom. Article 19 further implies the Limits on Content (or *Use*) and Degree of Interference (privacy and integrity of content) are further figures of merit for assessing Internet freedom. The international watchdog organisation, Freedom House, annually assesses[184] the state of Internet freedom. Its 2013 report[185] concludes that of the sixty countries assessed, thirty-four have "[…] experienced a negative trajectory" while sixteen experienced a "positive trajectory" since mid-2012.

Such measures might be termed characterisations of freedom from repression, especially when the use of the Internet is to air social grievances, organise opposition political forces, or merely to disseminate information which may be embarrassing to those in powerful societal positions. Members of this group have written much about the topics of Internet-mediated empowerment of citizens and their cyber-repression[186]. Westby has stated the issue boldly: *"The interests of the nation state against the rights of the individual are colliding, with ICTs being the tool of choice to assert power by both sides*."[187]

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

[184] Freedom House applies a three-pillared approach to capture the level of Internet and ICT freedom:

- Obstacles to Access—including infrastructural and economic barriers to access, legal and ownership control over Internet service providers (ISPs), and independence of regulatory bodies;
- Limits on Content –including legal regulations on content, technical filtering and blocking of websites, self-censorship, the vibrancy/diversity of online news media, and the use of ICTs for civic mobilisation;
- Violations of User Rights—including surveillance, privacy, and repercussions for online activity, such as imprisonment, extralegal harassment, or cyber attacks.

Their reports are available at http://www.freedomhouse.org/report-types/freedom-net#.VBB2dUhA140

[185] Freedom on the Net 2013, A Summary of Findings, p. 2. Available at http://www.freedomhouse.org/report/freedom-net/freedom-net-2013#.VBB6CUhA140

[186] H. Wegener, "Cyber Repression: Going Worse. What can be done?," Proceedings of the International Seminars on Planetary Emergencies, Erice, (2011), "The consequences of comprehensive censorship – cyber repression - are grave and cannot be overestimated. Citizens are cut off from important benefits of the information age, and receive a skewed view of world reality, condemning them to political immaturity. Massive cyber repression can alter the collective state of mind of a nation. The gravity of massive information suppression is at par with other variants of cyber crime and cyber conflict …".

[187] Westby, op.cit.

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[188].

While this tension is most easily cast with respect of the behaviour of nation States, the absence of central governance of the Internet together with its widely dispersed structure makes it possible for non-governmental organisations and corporate entities to significantly limit Internet freedom for targeted groups. The Internet has enhanced the power of non-State actors to such a degree that governments find it attractive to coerce corporations[189] to perform censorship functions, monitoring of use, etc.

A possible approach to balancing freedom of access on a global scale could be considered in countries with industries that produce Internet technology. The governments of such countries could prohibit or at least require reporting on the export of "[…] goods and technology that would assist a foreign government in acquiring the capability to carry out censorship, surveillance, or any other related activity through means of telecommunications, including the Internet".[190] While the efficacy of such measures is debatable, they highlight the complementary nature of actions by nation States and industries in establishing the limits of Internet freedom.

Like most lagging indicators of behaviour, these negative measures are only part of the story. Just as telling, although more difficult to quantify, are behaviours that advance the social and economic well-being of a society. Strict governance with an articulated aim to assure network stability, security, and resilience can suppress inventiveness, new network paradigms, and technological openness.

It cannot be surprising that the legitimate (collective) interests of nation states can collide with interests of individuals in cyberspace. These interests include but are not limited to protecting citizens from acknowledged harms such as preserving societal

[188] Wegener, ITU 2011, p. 46

[189] "The U.S. government threatened to fine Yahoo $250,000 a day in 2008 if it failed to comply with a broad demand for user data that the company believed was unconstitutional, according to court documents unsealed Thursday." *U.S. threatened massive fine to force Yahoo to release data*, Washington Post, 11 September 2014

[190] US House of Representatives, H.R.3605 - Global Online Freedom Act of 2011

(cultural) norms, prevention of heinous crime[191] and terrorism, preventing the disruption of critical societal infrastructure (including the Internet and other IT infrastructures), protecting legitimate State secrets, promoting the foreign policy of the state, and promoting national economic well-being especially by influencing externalities. Although the rules-of-the-road in promoting competing nation-state interests is well developed outside the cyber realm, in cyberspace confounding difficulties rise due to 1) the absence of harmonious legal frameworks governing behaviour in cyberspace and 2) gross, historically derived, cultural differences that abound in a global network that crosses many national boundaries.

An example may be illustrative. EU nations generally have strong proscriptions regarding content they define as "hate speech" or its representational equivalent[192]. These prohibitions have their roots in the deaths of multitudes during World War II. Some Moslem States likewise have similarly strong prohibitions regarding spreading other faiths[193] or spreading blasphemous representations in word or picture of the prophet Mohammed. In both cases, the prohibitions reflect strong cultural norms, the violation of which can lead to social discord and even violence. When governments block such sites, are they engaging in a repressive violation of human rights?

In contrast, the US takes an expansive view of what constitutes permissible speech that is enshrined in its constitution. The noted American legal scholar Lawrence Tribe (and his colleague) have written[194]:

> "Speech is powerful. It is the lifeblood of democracy, a precondition for the discovery of truth, and vital to our self-development. But speech is also dangerous. It can corrupt democracy, enable or incite crime, encourage enemies, and interfere with government. It can be wielded as a weapon and deployed against unwilling targets."

[191] International police cooperation to root out child pornography is a universally agreed upon example.

[192] For example, a French court got Yahoo! to drop Nazi paraphernalia from its auction site. Is that worse than China forcing Yahoo! to sign a "voluntary pledge" to refrain from "producing, posting, or disseminating pernicious information that may jeopardise State security and disrupt social stability? Christopher Bodeen, "Web Portals Sign China Content Pact," Associated Press, 15 July 2002.

[193] Hillary Clinton, "Internet Freedom," http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

[194] Lawrence Tribe and Joshua Matz, Uncertain Justice, (New York, 2014) p.123.

Yet even in the US limitations on speech to curb “hate speech” and “cyber-bullying” are becoming more commonplace. In the highly litigious American society, the limitations are still not prior restraints on speech, but rather grounds for torts or even criminal penalties.

Beyond physically blocking access to sites, governments may make access unacceptably costly with the effective intent of severely limiting access based on political considerations. For example, the surveillance of sites containing “dangerous” and/or provocative or illegal content in order to track and restrict those who visit such sites, may be followed by the application of secret procedures for the freedoms of persons visiting the sites. Many people have found themselves on no-fly lists due to faulty surveillance of “terrorist” sites. Although it is easy to admit to compelling State interests in such surveillance programmes, the lack of open judicial procedures to balance individual interests is troubling.

Significant disagreement between nations can be found in policies in the area of anonymity and privacy. Many perceive anonymity in Internet communications as a right. As anonymity may shield the speaker against harassment or retaliation, it is perceived as vital to freedom of speech. Indeed, the US recognises[195] a right to anonymous political campaigning; likewise they have affirmed a right to anonymous interactions between people “as long as those acts are not in violation of the law”.[196] Nonetheless, the US has not enacted broad policies regarding anonymity and privacy on the web, preferring to regulate specific industries. More aggressively, the EU has opted to directly regulate the privacy and anonymity rights of individuals.

In contrast, anonymity may be a convenient shield for disruptive and criminal behaviour. Among imposing other restrictions that tighten controls over the use of the Internet, Russia now prohibits anonymous access to Wi-Fi in public places[197] where the IP number cannot be definitively linked with specific individuals. Moreover, as shown by the Snowden revelations, the US government insists on an extremely broad (and perhaps unlimited) prerogative to track Internet communications. And it is not only governments which track Internet use – major corporate players such as Google

[195] US Supreme Court, McIntyre v. Ohio Elections Commission (93-986), 514 U.S. 334 (1995).

[196] "Decision *Columbia Insurance Company v. Seescandy.com, et al.* of the U.S. District Court in the Northern District of California".

[197] “Medvedev signs order banning anonymous Wi-Fi,” http://en.itar-tass.com/russia/744055, Aug. 8 2014

also track use extensively- Not surprisingly different users now see an individually tailored (or targeted) Internet experience, whether they want to or not.

The widespread US use of surveillance dragnets and monitoring communication of the heads of friendly governments, as revealed by the Snowden disclosures, suggest that few if any telecommunications are truly private. Unfortunately, full public debate of the extent, motivations, and rubrics of such State activities are typically hidden even from judicial review by claims of State secrets privilege[198]. The defence by the US government that "everybody does it" is hardly reassuring. Indeed, with the dramatic expansion of computer capabilities and data storage capacity per unit cost, virtually any industrialised State can monitor all Internet traffic entering or leaving a country. For the top economic tier of nations wholesale monitoring of all traffic is possible with the complicity (forced or voluntary) of telecommunications service providers.

The character of the public response both in the US and Europe to the revelation of nearly universal surveillance of cell phone traffic has led Apple to issue its most recent cell phone operating system (iOS8) with strong encryption with no backdoor. Thus, even Apple cannot decrypt a phone under court order.[199] While Apple's critics insist that iOS8 "only stops lawful investigations with lawful warrants,"[200] its defenders argue that Apple is "building systems that prevent everyone who might want your data–including hackers, malicious insiders, and even hostile foreign governments–from accessing your phone. This is absolutely in the public interest. Moreover, in the process of doing so, Apple is setting a precedent that users, and *not*

[198] "The state secrets privilege is an evidentiary rule created by United States legal precedent. Application of the privilege results in exclusion of evidence […] based solely on affidavits submitted by the government stating that court proceedings might disclose sensitive information which might endanger national security. *United States v. Reynolds*, which involved military secrets, was the first case that saw formal recognition of the privilege." http://en.wikipedia.org/wiki/State_secrets_privilege

[199] Apple privacy code: "Our commitment to customer privacy doesn't stop because of a government information request." https://www.apple.com/privacy/government-information-requests/ See also Matthew Green, "Is Apple picking a fight with the US government," Slate 23 September2014. Available at http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html

[200] Oren Kerr, "Apple's dangerous game," http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/Kerr has modified his views somewhat, recognizing that a system with an encryption backdoor is subject to hacking by anyone and thereby compromises the security of the system as a whole.

companies, should hold the keys to their own devices."[201] The official, institutional response of the US government remains to be seen; however, a succession of public officials has denounced[202] Apple's approach. An official, institutional response more coercive than moral persuasion would not be surprising.

The US has previously sought to impose requirements on hardware manufacturers to enable tracking, expose identities, and to decrypt Internet traffic. In describing how the US State Department works to "protect and defend a free and open Internet" as an element of its policy[203], Secretary Clinton has explained:[204]

> "All societies recognise that free expression has its limits. We do not tolerate those who incite others to violence, such as the agents of al Qaeda who are - at this moment – using the Internet to promote the mass murder of innocent people. And hate speech that targets individuals on the basis of their ethnicity, gender, or sexual orientation is reprehensible. It is an unfortunate fact that these issues are both growing challenges that the international community must confront together. We must also grapple with the issue of anonymous speech. Those who use the Internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities."

Yet, contemporaneously, the FBI. has warned Internet-cafe owners in the US "[…] that the use of certain basic cyber-security measures could be considered grounds for suspicion of possible terrorist activity".[205]

Similar tensions between individual and State interests are also found in the developing world, whereas in the industrialised world cryptography is considered to be a munition available to law-abiding citizens and criminals and terrorists alike.

[201] Matthew Green, Ibid.

[202] In an interview with the new CBS programme 60 Minutes on 12 October 2014, FBI Director James Carney charged that Apple's new privacy feature protects kidnappers, pedophiles and terrorists. See http://money.cnn.com/2014/10/13/technology/security/fbi-apple/index.html?hpt=hp_t2.

[203] US State Department, "International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World," http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[204] Clinton, op. cit.

[205] Vanity Fair, op. cit.

Within Africa, laws specifically pertaining to encryption seem to be limited to the North African States of Algeria, Egypt, Morocco and Tunisia, along with Nigeria and South Africa. In Africa, South Africa is at the forefront of cryptography law, yet the ethics of [the South African] key disclosure law is contested by some enthusiasts on the grounds of human rights. For some, cryptography seems to be the only solution to threats of privacy, as human society adapts to the digitalisation of world networks[206].

Presently strong, symmetric-key cryptography such at Open PGP is routinely available to anyone who does not reside in a terrorist-supporting State as designated by the US Department of State. It is difficult to imagine that actual terrorist cells are long deterred by that restriction. It is likewise difficult to imagine that proponents of military-grade encryption would find proposals requiring "voluntary escrow keys" to be deposited with the judicial arm of their home government[207] .

The potential for conflict between governments protecting what they see as legitimate interests of their respective citizens is manifest. Yet it is exactly where perceived offences cross multiple national borders that there may be little redress but for the aggrieved State to block the offending Internet Protocol (IP) address. The lack of harmonious legal frameworks governing behaviour in cyberspace is a serious obstacle. Even where the action in cyberspace is considered a serious crime in the State of the putative victim, the alleged perpetrator may be beyond the reach of the law[208].

[206] Cory Farmer and Judson L. Jeffries, "Telecommunications Surveillance and Cryptography Regulatory Policy in Africa," African Policy Journal, May 2013, available at http://apj.fas.harvard.edu/category/articles/

[207] "In this scenario copies of secret keys would be held behind layers of security in a dormant state, to be accessed only if proper warrants and decryption directions are granted." Cory and Farmer, Ibid, p.3

[208] For a country to investigate and prosecute, its law enforcement officials must be able to gather information and evidence in other countries. The fundamental obstacle to investigations where evidence and suspects are distributed across national borders is the need for law enforcement officials to respect the sovereignty of other countries. Law enforcement officials from one country typically may not enter another country to investigate leads, gather evidence and apprehend suspects. International investigations, accordingly, require the cooperation and assistance of authorities from the countries in which the victims, evidence and suspects are located. Even if suspects are identified, countries commonly will not allow extradition of their own citizens, instead asserting that domestic prosecution is proper, often on the grounds that extradition is inconsistent with their jurisdictional framework' would violate individual protections guaranteed to their citizens, and would lead to greater evidentiary obstacles at trial. Prosecutors, however, have found that countries that will not agree to extradite their own citizens do not consistently undertake domestic prosecution. G. A. Barletta, private communication, 201

When these interests of citizens are framed in the language of human rights rather than that of balancing competing legitimate interests, the stakes for both individuals and societies are raised. Engineer and Internet pioneer, Vint Cerf[209], has observed:

"[…] technology is an enabler of rights, not a right itself. There is a high bar for something to be considered a human right. Loosely put, it must be among the things we as humans need in order to lead healthy, meaningful lives, like freedom from torture or freedom of conscience. It is a mistake to place any particular technology in this exalted category, since over time we will end up valuing the wrong things".[210]

Unfortunately casting an Internet freedom (access) access as a human right provides the occasion in the political debate for the imposition of ideology over good sense. Whether in the form of "net neutrality" or "open access" for publications, both bandwidth and processing of content cost money. Too often ideologues have sought to guarantee "neutrality" and "access" as an unfunded mandate assuming that "someone else – usually the publisher – will pay" with an argument[211] frequently cast in terms of guaranteeing Internet freedom. Nonetheless, broad access and minimisation of infrastructure barriers are desirable goals that can be achieved in the context of many possible business models.

Industry has played a central role in both the creation and the governance of the digital society. The present freedom of action on the Internet is in great measure due to the insights of the private sector. While corporations are pressured by governments to abet repressive measures, they have also formed broad alliances with human rights groups, academics, investors, and civil society organisations to resist such pressures. A notable effort is the Global Network Initiative (GNI)[212]. The GNI has presented its vision[213] of the role of industry's "freedom of expression and privacy risk drivers." It notes that new technology (both hardware and software) and new security products are introduced at a rapid pace. These products bring both new risks and new opportunities with respect to Internet freedom. Although the industry has little direct

[209] Generally recognized as one of the "fathers of the Internet".

[210] V. Cerf, "Internet Access is Not a Human Right", New York Times, 4 January 2012.

[211] An example is the "op-doc" "A Threat to Internet Freedom," by B. Knappenburger, New York Times, 9 July 2014.

[212] https://globalnetworkinitiative.org/

[213] D.A. Hope, "Protecting Human Rights in the Digital Age," February 2011, http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf

control over the actions of the end users of technology it can provide the most technologically sophisticated advice to telecommunication service providers to minimise the incipient threats to Internet freedom.

The ICT industry has been increasingly proactive over the past few years in defining approaches to protecting freedom of expression and privacy. For example, the Global Network Initiative provides direction and guidance to companies on how to respond to government demands to remove, filter, or block content, and how to respond to law enforcement agency demands to disclose personal information. These types of risk drivers will be relevant for companies that hold significant amounts of personal information and/or act as gatekeepers to content, primarily telecommunications services providers and Internet services companies.

One can expect that as hardware evolves with strong security built in at the integrated circuit level, governments will exert ever stronger pressure on manufacturers to allow backdoor access to governments (low law enforcement and intelligence agencies) for surveillance, for tracking individuals, for tracing actions on the Internet and for securing evidence for judicial proceedings. Even more ominously, products could be developed and configured to enable censorship and content restrictions at the chip level. Although industries are at the focal point of pressures to restrict freedom, they are also the most knowledgeable and in a most advantageous position to thwart such pressures.

The rapid response of industry to the multiplying threats to the security of ICTs and the information that they generate, transmit, receive and store is a critical safeguard to the freedom of individuals and institutions to use digital information at will. Such freedom implies end-user confidence in the ownership[214], user rights[215], credibility[216] and privacy of data[217]. Some would also include in that list the ability to delete data from the Internet and legal safeguards against being coerced to reveal passwords of personal sites except under court order. The threats to freedom of use come from a wide variety of actors ranging from individual hackers to criminal groups to State-sponsored groups.

Assuring personal freedom on a resilient and secure Internet infrastructure will not happen by chance. Positive action must be taken to balance State interests against individual and private sector interests while at the same time protecting all users against malicious actors. The nature of State actions can be expected to take different forms in different societies.

In Western countries we would expect a central reliance on judicial review – whether confidential[218] or not – to rule on individual cases rather than providing mass authorisations to law enforcement and intelligence agencies. Active engagement of industry – both hardware manufacturers and software designers – would offer increasing levels of security and privacy for users. In concert, Internet service providers would confidentially manage the long-term capture and storage of user data

[214] The [putative] owners of information often claim legal protection of rights over dissemination and use of information. The owner may set the criteria or even the control of access to information. Such criteria may include rights to further dissemination by the authorised user (or user organisation). Such control is the practice with respect to security of State information, proprietary information, and personal confidential information. Oblique [and legalistic] attacks on ownership rights can lower the utility of information even to the point of making it non-actionable.

[215] The owner of the information may set the criteria for the use of information or even control of access to information. Such control is normal when the information is considered legally protected intellectual property.

[216] The user of the data should (and may be legally required to) assess (and perhaps document) his level of confidence of the data generator, source (provider), and the actual uncertainties in the data content (such as measurements, transactional records, statistics, etc.). Attacks on the credibility of information aim at reducing the utility of data, and undermining stakeholders confidence in the competence of the parties (and institutions) using that data.

[217] Of particular concern to individuals in the case of specific personal identification information.

[218] Such as the US FISA courts. Mere administrative commissions are insufficient.

accessible to government scrutiny only under clear and transparent conditions. There should be some rule of proportionality, the limitless fury of governmental net intrusion and data collection should cease, and intergovernmental cooperation in setting terms for spying on allies and agreements like the Safe Harbour Framework[219] should be developed. The actual legal framework should be the result of legislation informed by full, open public debate and consultation with allies and international bodies.

In contrast, China has constructed a distinct national Internet:

> "Not only has Chinese authoritarian rule survived the Internet, but the State has shown great skill in bending the technology to its own purposes, enabling it to exercise better control of its own society and setting an example for other repressive regimes. China's party-State has deployed an army of cyber police, hardware engineers, software developers, web monitors and paid online propagandists to monitor, filter, censor and guide Chinese Internet users. Chinese private Internet companies, many of them clones of Western ones, have been allowed to flourish so long as they do not deviate from the party line. […]
>
> The Chinese Internet resembles a fenced-off playground with paternalistic guards. Like the Internet that much of the rest of the world enjoys, it is messy and unruly, offering diversions such as games, shopping and much more. Allowing a distinctly Chinese Internet to flourish has been an important part of building a better cage. But it is constantly watched over and manipulated"[220].

As China sells its technology abroad in central and Southeast Asia, in Eastern Europe and Africa, it is gaining allies in its dispute with the US and the EU over Internet governance. The results of that dispute will likely set the boundaries of Internet freedom on a global scale.

[219] https://safeharbor.export.gov/list.aspx

[220] "China's Internet: A giant cage," The Economist, 6 April 2013

Table of Abbreviations

AFACT	Asia Pacific Council for Trade Facilitation and Electronic Business
APS	American Physical Society
ARPANET	Advanced Research Projects Agency Network
ASEAN	Association of Southeast Asian Nations
CAPTEL	Centre for Asia Pacific Technology Law and Policy
CBMs	Confidence-building measures
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEB	Chief Executives Board
CERN	Conseil Européen pour la Recherche Nucléaire
CERT	Computer Emergency Readiness Team
CIRT	Computer Incident Response Team
CIA	Confidentiality, Integrity and Availability
CoE	Council of Europe
COP	Child Online Protection Initiative (ITU)
CSCE	Commission on Security and Cooperation in Europe
EC3	European Cybercrime Centre (Europol)
EEAS	European External Action Service (European Union)
ENISA	European Network and Information Security Agency
EPFL	Ecole Polytechnique Fédérale de Lausanne
EU	European Union
EUROPOL	European Police Office
FBI	Federal Bureau of Investigation
G8	Group of Eight

GCA	Global Cybersecurity Agenda (ITU)
GDPR	General Data Protection Regulation
GGE	Group of Governmental Experts
GNI	Global Network Initiative
GPS	Global Positioning System
HLCM	High-Level Committee on Management
HLCP	High-Level Committee on Programmes
HLEG	High-Level Experts Group
HRC	Human Rights Committee (HRC)
IAEA	International Atomic Energy Agency
ICANN	Internet Corporation for Assigned Names and Numbers
ICSC	International Centre for Scientific Culture
ICT	Information and Communication Technology
INDECT	Intelligent Information System supporting observation, searching and detection for security of citizens in urban environment
IEC	International Electrotechnical Commission
IGF	Internet Governance Forum
IMPACT	International Multilateral Partnership Against Cyber Threats (Malaysia)
IP	Internet Protocol
ISF	Information Security Forum
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITIS	Institute for Intelligent Systems
ITU	International Telecommunication Union
ITU HLEG	International Telecommunication Union High-Level Experts Group

LDCs	Least Developed Countries
LINC	Lebanese Internet Center
LITA	Lebanese Information Technologies Association
MAC	Mandatory Access Control
MIT	Massachusetts Institute of Technology
NATO	North Atlantic Treaty Organization
NIS	Network and Information System Security
NSA	National Security Agency
OSCE	Organization for Security and Cooperation in Europe
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PMP	Permanent Monitoring Panel of Information Security (WFS)
RFID	Radio-Frequency Identification
SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrated Level
SLA	Service Legal Agreement
SMAC	Social, Mobile, Analytics and Cloud
SOA	Service Oriented Architectures
SORM	System for Operative Investigative Activities
TCP	Transmission Control Protocol
UAE	United Arab Emirates
UCLA	University of California, Los Angeles
UDHR	Universal Declaration of Human Rights

UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UN CEFAT	United Nations Economic Commission for Europe
UNDG	United Nations Development Group
UNDP	United Nations Development Programme
UN ESWA	United Nations Economic and Social Commission for Western Asia
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UNESCO	United Nations Educational, Scientific, and Cultural Organization
UNGA	United Nations General Assembly
UNGCE	United Nations Group of Government Experts
UNIDIR	United Nations Institute for Disarmament Research
UNODC	United Nations Office on Drugs and Crime
US-CERT	United States Computer Emergency Readiness Team
WFS	World Federation of Scientists
WIPO	World Intellectual Property Organization
WMD	Weapon of Mass Destruction
WSIS	World Summit on the Information Society

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

ISBN 978-92-61-15301-4
9 789261 153014

Price: 79 CHF

Printed in Switzerland
Geneva, November 2014

Photo credits: Shutterstock

11/2014