BARBARA WEEKES
ENEKEN TIKK-RINGAS

CYBER SECURITY AFFAIRS:
GLOBAL AND REGIONAL PROCESSES, AGENDAS AND INSTRUMENTS

GENEVA 2013
ICT4PEACE FOUNDATION

Barbara Weekes, Eneken Tikk-Ringas (2013) Cyber Security Affairs: Global and regional Processes, Agendas and Instruments, ICT4Peace Publishing, Geneva.

Copies available from www.ict4peace.org.

INTRODUCTION

The world is facing a new challenge that is here to stay: an invasive, multi-pronged and multi-layered threat, a modern day arms race without visible weapons or actors, characterized by an escalating number of attacks both on and off the radar. The stability of our networked global system and the proper functioning of our countries, cities and daily activities, rely on the Internet. Critical infrastructure – including transport, transport security, nuclear power plants, electricity, communication networks, oil pipelines, and financial institutions – has become a clear target for cyber attacks, which could have devastating consequences for humankind.

The Internet is a global common good, which has triggered an explosion of innovation, entrepreneurial spirit, communication, business activity, economic growth, social networking, and exchange of ideas. Tackling a threat to this mainstay of modern society requires a global effort, a concerted open dialogue to find common ground and solutions.

While these activities have been taking place for many years behind the scenes, the recent increased number and frequency of media reports, citizens are becoming increasingly aware of this new threat to their wellbeing and are looking towards their governments, civil society leaders and business to engage at the national and global level to find solutions and international agreements to mitigate this threat.

Building on the World Summit on the Information Society (WSIS) and keeping in mind the United Nations Millennium Declaration on peace, security and disarmament, Nation states need to push the international cyber agenda ahead, placing a priority on cyber diplomacy both at a multilateral and bilateral levels. The cloak and dagger erosion of trust currently taking place within countries and between countries at the highest level needs to be stopped through increased transparency and trust building. Cyber-cooperation and cyber diplomacy should become the norm.

There are encouraging signs that States are finally engaging (e.g at the UN, OSCE, ARF), but more robust and output oriented negotiations are needed. Admittedly this is a new area for diplomats and the relevant stake-holders. It is for that reason that the ICT4Peace Foundation has decided to publish this map of global and regional Processes, Agendas and Instruments that are addressing the issue of cyber security. We wish to thank the Swiss Ministry of Foreign Affairs for their support to the writing of this report.

Daniel Stauffacher
President
ICT4Peace Foundation

THE UNITED NATIONS

Main areas of focus and impact: crime, international peace and security

Secondary areas of focus and impact: human rights

The main current processes in the UN include the Group of Governmental Experts convening under the auspices of the First Committee to address threats to international information security as the outcome of the work of this group reflects consensus among the Permanent Five about what is regarded as a potential threat to international peace and security and what measures expected are expected to be taken by member states to build confidence in peaceful uses of ICTs and, in case of a conflict, prevent escalation.[1]

Also, a still pending proposal on a new international treaty on cyber crime deserves attention and perspective assessment from strategic level 'cyber security' communities as this reflects the potential of criminal cooperation on a global level.

National views on international information security are requested yearly under the information security initiative in the First Committee.

The Disarmament and International Security Committee (the **First Committee**) has looked into the developments and uses of technology since the late 1990s. The use of information and communication technologies[2] became its focal point from a politico-military perspective in conjunction with the Russian draft Resolution from 1998 on the Developments in the Field of Information and Telecommunication in the Context of International Security.

Since then the Resolution has been passed yearly with Russia and the Shanghai Cooperation Organization countries as the main sponsors. Three groups of governmental experts have been called to consider existing and potential threats in the sphere of information security, possible cooperative measures, and to conduct a study of international information security issues. Yearly national contributions address concerns and proposals on global information security.[3]

The Russian initiative has been counterbalanced by the US whose goal has been to expand the discussions of 'cyber security' on combating the criminal misuse of information technologies and law enforcement in the **Third Committee**[4] and 'a global *culture of cybersecurity*'[5] in the **Second Committee**. The concepts of the Second Committee are further pursued in the framework of IGF (covered later in this study).

Cyber crime has been on the agenda of the UN since 1990 when the first resolution on computer crime legislation was adopted at the Congress on the Prevention of Crime and Treatment of Offenders.[6] UN Manual on the Prevention and Control of Computer-Related Crime followed in 1994.

At the **UNODC** Expert Group on Cybercrime[7] session in Vienna in January 2011 Russia initiated a discussion on a new convention on cybercrime. Russia has been concerned with the Budapest Convention as

1 The first GGE met 2004-2005 and the second GGE 2009-2010. The meetings of the third GGE are scheduled to August 6-10, 2012 (New York), January 14-18, 2013 (Geneva) and June 3-7, 2013 (New York).

2 The term „use of ICTs" has been adopted to scope key concerns and remedies of international information security.

3 See in more detail Tikk-Ringas (2012).

4 See A/RES/55/63, A/RES/56/121.

5 UN General Assembly resolution 57/239 (2002) outlined elements for creating a global culture of cybersecurity, inviting member states and all relevant international organizations to take account of them in their preparations for the WSIS. UN resolution 58/199 (2003) further emphasized the promotion of a global culture of cybersecurity and the protection of critical information infrastructures.

6 UN/A/RES/45/121.

7 The mandate of this group is to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime (ECOSOC resolution 2010/18 and by the Genral Assembly in its resolution 65/230).

unable to provide systematic response to the new trends of cybercrime and 'cyber terrorism'. Russian argumentation on the absence of codified notions of cybercrime and cyber terrorism and the lack of conceptual criminalization at the international level has been supported by China, Brazil and selected African countries. Following the Russian proposal an International Expert Group was tasked to conduct a thorough study on cyber security. The report was delivered in early 2013.

The scope and emphasis of developing a new international instrument is still open as the initiative on a new treaty is pending the conclusions to be reached by the intergovernmental expert group[8], who tabled a comprehensive study of the problem of cybercrime in March 2013[9]. The likelihood that eventually a new instrument will be drafted is there as more and more of a push for some kind of treaty at the UN level from an increasing number of nations. In addition, the area of cyber crime is a less sensitive area for norm development than international peace and security.

The coalition of countries demanding clarity of norms applicable to cyber security is spear-headed by Russia and China. On September 12th 2011 four countries: China, the Russian Federation, Tajikistan and Uzbekistan submitted a letter to the Secretary General of the United Nations[10]. Annexed to this letter was a draft code of conduct for information security.

The purpose of the Code is to identify the rights and responsibilities of states in the information space. The scope is similar to the document proposed by the Council of Europe in a document titled Internet Governance Principles and also reflects the thinking underlying the Shanghai Cooperation Organisation's information security agreement and the Concept Convention on International Information Security. The code is meant to be a non-binding instrument and open to all the states. The proposed Code of Conduct has faced rejection by the coalition of the like-minded liberal democracies, primarily because of the interpretation of it as an attempt to establish new binding obligations and emphasizing state sovereignty over the multi-stakeholder Internet governance model.

UNIDIR has engaged in event co-hosting and reporting with the German and the U.S. governments, has studied military cyber capabilities of countries and has been considered as a venue for further studying the applicability of international law to the uses of ICTs for the purposes of the First Committee process.

While the Security Council has so far abstained from discussing cyber security issues, a task force has addressed aspects of cyber terrorism. The Counter-Terrorism Implementation Task Force (**CTITF**) was called by the Secretary-General in 2005. In 2011 the Task Force published a compendium on Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects[11], predated by a report on the same topic in 2009.

WSIS was started by the UNGA (Resolution 56/183) and hosted by ITU.[12] The first phase of the Summit was held in Geneva in December 2003 and the second phase in Tunis in November 2005. The WSIS Declaration of Principles[13] call for a global culture of cybersecurity to strengthen information security and network security, authentication, privacy and consumer protection, and for building confidence among users of ICTs.

In accordance with its mandate, the UN has discussed a variety of cyber security topics and issues, but largely without groundbreaking outcomes or influence. National input to the First Committee process indicates significant differences in understanding and emphasis on the issue. Although some countries have indicated the

8 Established under General Assembly Resolution 65/230.

9 Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice systems and Their Development in a Changing World.

10 United Nations General Assembly A/66/359.

11 http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_ 2011.pdf.

12 http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_56_183.pdf

13 http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160

UN as the best potential guarantor of global cyber security, such proposals have remained below a global consensus threshold.

INTERNATIONAL TELE-COMMUNICATIONS UNION (ITU)

Main areas of focus and impact: technical security, information infrastructure standards

Secondary areas of focus and impact: CII, crime

ITU has played a role in the security of telecommunications for decades. After having been appointed to support WSIS and considering the 1989 version of the International Telecommunication Regulations that addressed the trend of private telecommunication services, ITU has assumed a more strategic role in the field of Internet governance and global cyber peace. While ITU's increasing authority over the Internet is welcomed by many states, it has been conceptually rejected by many liberal democracies.

The ITU is the United Nations specialized agency for information and communication technologies. In addition to the 193 Member States, ITU membership comprises ICT regulators, academic institutions and some 700 private companies. ITU has been promoted by the Russian-Chinese contingent as the multi-stakeholder organization best suited to address Internet Governance.

The ITU, under its Constitution, was established to maintain and extend international cooperation among all its Member States for the improvement and rational use of telecommunications of all kinds. ITU Constitution includes provisions on stoppage and suspension of telecommunication services.

The International Telecommunication Regulations adopted in 1989 and revised at the ITU Dubai Plenipotentiary in December 2012 have been referred to as empowering the ITU with the supervision of the security of the Internet. While the topic of privatization of telecommunication services was discussed and considered in 1989, the legal status of ITRs is hardly strategic. The 2012 plenipotentiary failed to reach consensus on ITU's role in Internet governance.

The launch in 2007 by ITU Secretary-General, Dr. Hamadoun I. Touré, of the ITU Global Cybersecurity Agenda (GCA) came as a surprise to those countries who had regarded ITU as primarily a technical and standardization agency. ITU has promoted GCA as a framework for international cooperation aimed at enhancing confidence and security in the information society. WSIS[14] and the 2006 ITU Plenipotentiary Conference refer to a mandate for the ITU of coordinating international efforts in the field of cyber security.

In 2011 the ITU concluded a strategic alliance with the International Multilateral Partnership Against Cyber Threats (IMPACT). IMPACT hosts the ITU GCA and provides States access to expertise, facilities and resources to effectively address cyber threats, as well as assisting United Nations bodies in protecting their Information and Communication Technologies (ICT) infrastructures.[15] The IMPACT/GCA initiative of the ITU has received wide acceptance from the international community[16] but has been less welcomed by the U.S. and the like-minded.

INTERNET GOVERNANCE FORUM (IGF)

Main areas of focus and impact: Internet governance, information society development

Secondary areas of focus and impact: human rights

Despite its marginal role in strategic level decision-making and concept development about national and international security concerns IGF still offers a useful networking and representation base for addressing economic and social aspects of Internet governance. However, IGF has not been used by

14 http://www.itu.int/wsis/

15 http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html

16 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT_AnnualBook.pdf

the leading governmental powers to propose new initiatives or discuss strategic issues.

The Internet Governance Forum (IGF) is an open forum without fixed membership. The second phase of WSIS requested the Secretary-General of the United Nations to convene 'a new forum for a multi-stakeholder dialogue'.[17] The mandate of the IGF is to discuss the main public policy issues related to Internet governance in order to foster the Internet's sustainability, robustness, security, stability and development.

After a series of successful meetings started in 2006 the United Nations General Assembly extended the IGF's mandate for five years in 2010.

Recently, the margin of usefulness of the IGF has received different assessments from governments. The forum is perceived as useful for information society related discussions and coordination as it brings together initiatives and experience from various international organizations and governments. At the same time, it has been referred to as largely ignorant of emerging security concerns. With national security interests increasingly surrounding Internet governance issues, the role of the IGF has gradually decreased, but can resume again depending on national initiative invested.

G8

Main areas of focus and impact: CII, cyber crime

The G8 has been used as a restart platform for emphasizing the need to deal with cyber security from a strategic perspective. However, its role in shaping multilateral discussions is mainly declarative given the principal differences between the U.S., Russia and China on the next steps needed to stabilize international cyber security affairs.

The Group of Eight first addressed information security in the communiqué of the Meeting of Justice and Interior Ministers in 1997 with emphasis on investigating and prosecuting high-tech crimes and strengthening international legal regimes for extradition and mutual legal assistance. G8 countries have also attended to the threat of the convergence of cybercrime and terrorist activity.

In Deauville 2011 the governments reaffirmed the need for coordination of the security of networks and services on the Internet.[18]

COUNCIL OF EUROPE (COE)

Main areas of focus and impact: human rights, cyber crime

Secondary areas of focus and impact: Internet governance, cyber terrorism

The activities of the Council of Europe are most valuable from the perspective of updating national criminal law and following the trends in investigating and prosecuting cyber incidents. The impact of the Budapest Convention is supported by a platform the Council of Europe has developed with the European Union. However, given the principal resistance to the Convention by a group of countries including Russia, Brazil and South Africa, the impact of the European Union has decreased in this niche.

Although the Council of Europe is best known in the area of cyber security for its Convention of Cybercrime (also known as the Budapest Convention), it was the first international organization to address the issue of **automated data processing and privacy** in 1981[19]. It therefore has an important role in guaranteeing the independence of national data protection authorities. The COE has also looked into the issue of cyber terrorism.

The **Budapest Convention**, adopted in 2001, is often at the core of cyber security discussions and

17 http://www.un.org/News/Press/docs/2006/sga1006.doc.htm

18 G8 DECLARATION: RENEWED COMMITMENT FOR FREEDOM AND DEMOCRACY (G8 Summit of Deauville - May 26-27, 2011)

19 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981

legal questions about the sufficiency and adequacy of international law are often raised with reference to the Convention as the, so far, sole document addressing "cyber". Such an approach is legally ill-grounded as the Convention addresses only international criminal cooperation in the field of computer and network security. Under Article 27 it is not applicable in cases where national security interests are involved.

As recently several states have suggested that the Convention needs updating as it does not adequately respond to all the new threats and challenges, several studies on the subject have been conducted.[20,21,22]

The main challenges include cross-border forensics, jurisdiction and illegal access to data stored in the cloud, a set of issues possible to be resolved by an additional protocol. The US has been against any changes in the Convention.

Cyber crime related questions have been discussed within the Cybercrime Convention Committee (T-CY). The T-CY started to work with the subject in 2009, focusing on issues like jurisdiction and trans-border access to data and data flows.[23]

CODEXTER, established in 2003 to strengthen legal action against terrorism and safeguard fundamental values and address the causes of terrorism, has discussed the issue of cyber terrorism and concluded that:

"The existing international conventions and other instruments that promote the harmonization of national substantive and procedural law and international cooperation are applicable to these misuses of the Internet for terrorist purposes: The computer-specific provisions of the Council of Europe's Cybercrime Convention that address national substantive law, national procedural law, and international cooperation can be used in cases of terrorism.

Furthermore, the substantive and procedural rules as well as the rules on international cooperation found in international instruments on terrorism, on money laundering and financing of terrorism, and on general mutual assistance and extradition are also applicable in the cyber terrorism context."[24]

In 2006, the COE launched its Global Project on Cybercrime focused on global capacity building in the field. The **Octopus Interface** is a format for discussing the Budapest Convention implementation. Yearly events since 2007 elaborate on cybercrime threats and trends, national policies and initiatives on cybercrime.

The Council of Europe has also looked into the issue of Internet Governance, seeking to combine some IGF considerations with the ideas of the European Convention of Human Rights. In 2011 a package of Internet Governance Principles[25] was introduced containing a set of principles on the protection and promotion of the universality, integrity and openness of the Internet[26].

20 Cybercrime and Internet jurisdiction. Discussion paper prepared by Prof. Dr. Henrik Kaspersen http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

21 Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers. Prepared by Joseph J. Schwerha IV http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

22 Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Prepared by Jan Spoenle. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

23 Ad hoc sub-group of the T-CY on jurisdiction and trans-border access to data and data flows. Draft Terms of Reference. T-CY (2011) 5 E http://www.coe.int/t/dghl/standardsetting/t-cy/tcy2011/TCY_2011_5E_BU_draft_tor_crossborder_v3.pdf

24 See CODEXTER (2007) cyberterrorism and other use of the internet for terrorist purposes – Threat Analysis and Evaluation of International Conventions

25 Declaration by the Committee of Ministers on Internet governance principles was adopted by the Committee of Ministers on 21 September 2011. https://wcd.coe.int/ViewDoc.jsp?id=1835773&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

26 Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet. Adopted by the Committee of Ministers on 21 September 2011 https://wcd.coe.int/ViewDoc.jsp?id=1835707&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

THE EUROPEAN UNION

Main areas of focus and impact: technical security, information infrastructure, information society, e-commerce, cyber crime

Secondary areas of focus and impact: national security

The impact of the European Union in the field of international cyber security is defined by a harmonized level of cyber security in Member States (and the EEA) deriving from the numerous information society related instruments. The upgrade of relevant criminal law represents a valuable addition to any country's cyber crime arsenal. The work of ENISA has recently intensified and the agency has issued valuable guidance on CERT cooperation and cyber incident handling, also of strategic national relevance.

The EU Joint Communication on a European Strategy on Cybersecurity adopted in March 2013 indicates shared views and values of the like-minded and the balance of interests between the EU countries. It is difficult to assess the practical impact of the document at this point as several man goals remain declaratory and indicate need for further balancing, e.g. between privacy and security goals.

The priority objectives for the European Union (EU) in the field of cyber security have long been the common market and related information society aspects as well as cybercrime. The European Network and Information Security Agency (ENISA) serves as the mandated agency for the European Union, the EU Member States and the business community.

The EU has approached the issue of cyber security from rather different angles, often in a defragmented and even competing manner. The EU's main contribution to its member states cyber security has been a harmonized level of preparedness to defend against cyber attacks resulting from numerous directives and decisions addressing security measures, required levels of security and practices for securing and maintaining information systems and services.

On the politico-military side, the EU has contributed to the mostly regional dialogue on critical infrastructure protection and cyber terrorism. In the past five years the European discussion on cyber security has comprised cyber defence from a military perspective.

The fight against cybercrime has been a priority for European Union for a long time with dozens of directives having been adopted on various aspects of uses of ICTs and development of information society.

On 30 September 2010, the European Commission published a new draft directive on attacks against information systems, repealing the Council Framework Decision 2005/222/JHA[27] to update the cybercrime legislation of the EU and replace the older Framework Decision.

The European External Action Service (EEAS), created under the Lisbon Treaty in 2009 is a diplomatic corps supporting the post of a new foreign affairs chief (Catherine Ashton from the U.K.) heading the European Union's international diplomacy. The role of the European External Action Service is to support the High Representative in fulfilling his/her mandate to conduct the EU's Common Foreign and Security Policy. One of the tasks undertaken by the EEAS was preparing the Communication on European Strategy for Cybersecurity. This document was tabled in February 2013.

The strategic objectives of this initiative are to overcome national fragmentation and support Member States in their efforts to ensure safe and resilient digital environment for all EU citizens, businesses and public administrations, to effectively prevent cybercrime, in respect of human rights and European values, and to ensure concerted EU international activities in order to safeguard the EU's interests in the field of cyber security.

27 COM(2010) 517 final http://eur-lex.europa.eu/Result.do?T1=V5&T2=2010&T3=517&RechType=RECH_naturel&Submit=Search

The EU Strategy comprises legislative proposals to addressing minimum capabilities required to mitigate threats. The strategy is intended to re-establish trust of the Internet among Europeans and will address cooperation on both strategic and technical levels.

OECD

Main areas of focus and impact: human rights, e-commerce

Secondary areas of focus and impact: crime, CII

As observed by Klimburg and Tiirmaa-Klaar[28], cybersecurity in the OECD context has predominantly been a sub-category of economic and technology policy and for that reason the rise of cybersecurity as a subject for national security has somewhat reduced its importance for the OECD's agenda.

The OECD has been engaged in privacy and computer-related crime from early on and was one of the first organizations to examine computer related crime. With shared values on pluralistic democracy, respect for human rights and market-oriented economies, the OECD's main focus in the field of cyber security is on its economic and societal aspects. The impact of the OECD on the strategic threads of cyber security is increasing in light of the controversies surrounding the topic of Internet Governance.

OECD Guidelines on Privacy were adopted and became effective in September 1980 and have been used in the development of laws and policies in a number of OECD countries, including Japan and Australia. As noted by the chairman of the Committee in charge of drafting the guidelines, as compared to the Council of Europe Convention the guidelines, aimed at being less 'European' in orientation.

The OECD's Intergovernmental Working Party on Information Security and Privacy (WPISP) develops policy recommendations and reports in the field of information society and resilience building. The OECD's regular reports analyzing the impact of technology on information security and privacy as well as the OECD report on critical information infrastructure protection practices among its Member States are well-established sources of best practices, organizational structures and regulations.

In 2011, the OECD invited a study on Future Global Shocks including a sub-study on Reducing Systemic Cybersecurity Risk, published in 2012.[29]

OSCE

Main areas of focus and impact: crime, terrorism, international peace and security

Secondary areas of focus and impact: CII

OSCE has paid extensive attention to the issues of cyber crime and cyber terrorism and was one of the first organizations emphasizing the need for a comprehensive approach to cyber security. Recently, OSCE has undertaken to develop confidence-building measures (CBMs) to reduce the risks of conflict stemming from the use of information and communication technologies.

OSCE started discussions on strategic cyber security in 2008, with support from the Estonian Chairmanship of the Political and Security Committee. Previously, it had focused mostly on combating cyber crime and terrorism. In June 2010, the U.S. proposed a discussion on norms for state behavior in cyberspace.[30] After a short deliberation of options, the strategic cyber security agenda now focuses on confidence building measures (CBMs) in cyberspace.

On the Ministerial Council level Internet and cyber security issues are reflected in the OSCE Charter

28 http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf

29 http://www.oecd.org/sti/futures/globalprospects/46889922.pdf

30 See Schneider, Deborah, 'Cyber Security Keynote Address for the U.S. Department of State', United States Mission to the OSCE, 9 June 2010, http://www.osce.org/fsc/68524.

on preventing and combating terrorism.[31] The Parliamentary Assembly has adopted resolutions and declarations related to cybercrime and cyber security at different meetings.

Enhancing cyber/ICT security is a cross-dimensional and multifaceted endeavor in the OSCE. For a number of years already the Organization's Action against Terrorism Unit (TNT/ATU) and its Strategic Police Matters Unit (TNT/SPMU) focused on awareness-raising and capacity-building activities in their related fields and promoted a comprehensive approach to cyber security - The Representative on Freedom of the Media (RFoM) and the Office for Democratic Institutions and Human Rights (ODIHR) have also done relevant work.[32]

OSCE was one of the first organizations to refer to a 'comprehensive cyber security' agenda distinguishing between (a) the politico-military domain, including critical infrastructures, and (b) cybercrime and terrorist use of the Internet.[33]

Despite a considerable contribution to the cyber security agenda the role of the OSCE has remained somewhat debated due to the reluctance of the liberal democracies headed by the U.S. to elaborate a binding set of norms on State behavior. Instead, the OSCE is currently mandated to elaborate proposals on Confidence Building Measures. OSCE process on CBMs in cyberspace will indicate consensus platform between largely European countries and the balance of interests between the US and Russia.

OSCE is increasingly regarded by many nations as a forum with high potential for constructive cyber security discussions. It is believed that this is an area where the OSCE has a lot of unique expertise and where the Organization can fill an existing gap in international efforts related to cyber security. Of course, what countries discuss at the OSCE level should then, ideally, also feed into what they discuss elsewhere, including at the global level, i.e. the UN.[34]

31 http://www.osce.org/mc/42536

32 Input from OSCE officials.

33 9.-10.05.2011 A Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role. http://www.osce.org/event/cyber_sec2011

34 From interview with an OSCE official

NATO

Main areas of focus and impact: national security, international peace and security

Secondary areas of focus and impact: CII

NATO's main aim for 2012-2013 has been developing the operational capability of NCIRC, a CERT-like entity providing NATO agencies with information systems and network security services, and implementing its cyber defence policy adopted in 2011. NATO has also reorganized its information security agencies and created an umbrella organization in charge of both internal and cross-alliance information and communications systems.

NATO's deeper engagement in 'cyber defence' issues started with the decision in 2003 to develop a cyber defence expertise within the CCD COE (Cooperative Cyber Defence Centre of Excellence), finally established in Tallinn, Estonia in 2008.

Due to politically motivated cyber attacks against Estonia in 2007 and following the initiative of Estonia, France, the U.K. and the U.S., the North Atlantic Council and the Military Committee ordered the development of a NATO Cyber Defence Policy[35] and a NATO Cyber Defence Concept[36].

The NATO Cyber Defence Management Authority (CDMA) Board has the main responsibility for coordination and strategic decision-making on cyber defence within the Alliance. The newly established Emerging Security Challenges Division coordinates political and strategic oversight for NATO cyber defense efforts. The NATO Computer Incidence Response Capability Technical Centre serves as a central technical authority on operational cyber defense issues.[37]

The Lisbon Summit committed NATO and the Allies to addressing the new security challenges and, among other objectives, draws a very ambitious

35 A restricted document

36 A restricted document

37 http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf

roadmap for the cyber agenda of the Alliance. It includes bringing all NATO military and civilian bodies under central protection, introducing the cyber component to the defense planning process and accelerating information sharing and early warning capabilities.[38]

In 2010 NATO started a revision of its Cyber Defence Policy and the new Policy was adopted in June 2011.[39]

OAS[40]

The Organization of American States has been supported in its cyber security related activities by the US Department of Justice. The work in the region comprises of yearly cyber security conferences focusing mainly on law enforcement issues and CERT cooperation. OAS is planning a separate initiative for the Caribbean members. Training of judges and prosecutors is one of the most urgent needs. Brazil has been supporting the RU/CH narrative in the UN and on a bilateral basis.

AG/RES. 2004 (XXXIV-O/04): Adoption of a comprehensive Inter-American strategy to combat threats to Cybersecurity: A multidimensional and multidisciplinary approach to creating a culture of Cybersecurity.

AU[41]

The African Union has adopted a convention on cybersecurity with assistance from ITU.[42] The Draft Convention seeks to harmonize African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cyber crime control. It defines the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa. The Republic of South Africa has been supporting the RU/CH narrative in the UN and on a bilateral basis.

ASEAN[43]

Cyber security issues have been addressed by the ASEAN Political-Security Community and the ASEAN Economic Community.

The ASEAN Regional Forum in 2012 convened a special workshop on confidence building measures (CBMs) in cyberspace. Seen as an important regional factor in shaping the UN discussion of CBMs, ASEAN is currently setting up an initiative to develop a regional package of such measures.

SCO[44]

SCO has over the past years produced a package of information security related declarations and instruments. The Bishkek Declaration[45] reflected concern over the threat of using ICTs for purposes inconsistent with the tasks of protecting international stability and security; the Dushanbe Declaration[46] (2008) referred to the importance of activities in the fields of information technology and telecommunications in the context of international security, and the Yekaterinburg Declaration[47] (2009) highlighted the significance of ensuring international

38 NATO, Developing NATO's cyber defence policy, 25 January 2011, http://www.nato.int/cps/en/natolive/news_70049.htm

39 A restricted document

40 The OAS brings together all 35 independent states of the Americas and constitutes the main political, juridical, and social governmental forum in the Hemisphere

41 The African Union consists of 54 African states. The only all-African state not part of the AU is Morocco

42 Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

43 The Association of Southeast Asian Nations (ASEAN) was established in 1967 and currently it consists of ten Southeast Asian countries

44 The Shanghai Cooperation Organisation (SCO) is a permanent intergovernmental international organisation which was established in 2001 by the Republic of Kazakhstan, the People's Republic of China, the Kyrgyz Republic, the Russian Federation, the Republic of Tajikistan and the Republic of Uzbekistan

45 http://www.sectsco.org/EN/show.asp?id=92

46 http://www.sectsco.org/EN/show.asp?id=90

47 http://www.sectsco.org/EN/show.asp?id=87

information security as one of the key elements of the common system of international security. The Tashkent Declaration (2010) emphasized that information security is closely linked to ensuring state sovereignty, national security, social and economic stability and the interests of citizens. The Astana Declaration[48] (2011) notes that the emerging real threats to information security are causing grave concern.

An Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security was signed in Yekaterinburg on 15 June 2009. This instrument represents the SCO league's approach to norms development and supports the Russian and Chinese initiatives to draft a new treaty for cyber security.

ECOWAS[49]

ECOWAS has adopted the Directive on Fighting Cybercrime (2009) that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law. The Directive deals with offences specifically related to ICT, incorporating traditional offences into ICT offences and sanctions for such offences.

APEC[50]

APEC's Cybersecurity Strategy[51] was approved at the APEC Telecommunications and Information Working Group meeting in 2002. In 2005 the Lima Declaration[52] stressed the importance of ensuring the security and integrity of the APEC region's communications infrastructure, in particular the Internet, in order to bolster the trust and confidence of users and enable the continued advancement of this infrastructure. The Declaration was accompanied by the Key Principles for Broadband Development in the APEC Region; the Compliance and Enforcement Principles; the Guiding Principles for PKI-based Approaches to Electronic Authentication and the Principles and Implementation Guidelines for Action Against Spam.

Also in 2005, APEC Economic Leaders adopted the APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment[53].

APEC TEL Strategic Action Plan: 2010 – 2015 is the main policy outline for cybersecurity and cybercrime.

48 http://www.sectsco.org/EN/show.asp?id=294

49 The Economic Community Of West African States (ECOWAS) is a regional group of fifteen countries, founded in 1975. Its mission is to promote economic integration

50 Asia-Pacific Economic Cooperation (APEC) is a forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific region

51 http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012298.pdf

52 http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel.aspx

53 http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx

ICT4Peace
www.ict4peace.org

ICT4Peace was launched as a result of the World Summit on the Information Society in Geneva in 2003 and aims to facilitate improved, effective and sustained communication between peoples, communities and stakeholders involved in conflict prevention, mediation and peace building through better understanding of and enhanced application of Information Communications Technology (ICT). The ICT4Peace Cyber Security Program was started in 2011. We are interested in following, supporting and leading bilateral and multilateral diplomatic, legal and policy efforts to achieve a secure, prosperous and open cyberspace. The first phase of ICT4Peace activities in the field involves briefing of key processes shaping approaches to international cyber security.

Barbara Weekes

Barbara Weekes is a Senior Advisor of the ICT4Peace Foundation and the CEO of the Geneva Security Forum. Barbara also works in close collaboration with Dr Stauffacher + Partner Consulting, Zurich-Geneva, on various strategic advisory projects. As lead of the global affairs team at the World Economic Forum she was a key person in the development and execution of the program for the Annual Meeting in Davos from 1995 to 2000, in addition to designing the programs for the World Economic Forum´s Southern Africa Economic Summits in Capetown, Windhoek and Harare. Prior to her work at the World Economic Forum, Barbara was a member of the policy staff at the Department of Foreign Affairs and International Trade, Canada responsible for the preparation of the G-7 Summit in Halifax, 1995.

Eneken Tikk-Ringas

Eneken Tikk-Ringas is the Senior Fellow for Cyber Security at the International Institute for Strategic Studies based out of the Middle East office in Manama, Bahrain and serves as special advisor to ICT4Peace. Before joining IISS, Eneken worked as legal adviser and the head of the legal and policy team at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Eneken serves as international research associate at the Georgetown University Center for Law, Technology and Security and has long teaching experience in the field of ICT security, law and policy. She holds a PhD in law from the University of Tartu in Estonia. Eneken has written numerous articles on strategic cyber security issues, is a frequent speaker at international cyber security conferences and serves as assistant expert in the UN Disarmament and International Security Committee's Group of Governmental Experts.

ICT for peace
FOUNDATION