ICT for peace FOUNDATION

CYBER POLICY PROCESS BRIEF

# BASELINE REVIEW

## ICT-RELATED PROCESSES & EVENTS

IMPLICATIONS FOR INTERNATIONAL AND REGIONAL SECURITY

(2011-2013)

Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas

**GENEVA 2014**

ICT4PEACE Foundation

ICT4Peace Publishing, Geneva.

Copies available from www.ict4peace.org

INTERNATIONAL CYBER SECURITY

# BASELINE REVIEW

## ICT-RELATED PROCESSES & EVENTS

IMPLICATIONS FOR INTERNATIONAL AND REGIONAL SECURITY

(2011-2013)

Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas

ICT for peace FOUNDATION

# TABLE OF CONTENTS

1. BACKGROUND & INTRODUCTION ........ 8

2. INTERNATIONAL AND REGIONAL SECURITY ........ 10

2.1 INTERNATIONAL SECURITY ........ 10

2.2 REGIONAL SECURITY ........ 15

2.2.1. ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE) ........ 16

2.2.2. NORTH ATLANTIC TREATY ORGANISATION (NATO) ........ 16

2.2.3. EUROPEAN UNION ........ 18

2.2.4. ASEAN REGIONAL FORUM ........ 19

2.2.5. SHANGHAI COOPERATION ORGANISATION (SCO), COLLECTIVE SECURITY TREATY ORGANISATION (CSTO) AND COMMONWEALTH OF INDEPENDENT STATES (CIS) ........ 20

2.2.6. ORGANISATION OF AMERICAN STATES (OAS) ........ 20

2.2.7. AFRICAN UNION ........ 21

3. BILATERAL EFFORTS IN THE FIELD OF INTERNATIONAL AND REGIONAL SECURITY . 22

4. TRANSNATIONAL CRIME AND TERRORISM ........ 25

4.1 AN INTERNATIONAL CONVENTION ON CYBERCRIME? ........ 25

4.2 OTHER CYBERCRIME-RELATED MEASURES, PROCESSES & DEVELOPMENTS ........ 28

4.3 INTERNATIONAL EFFORTS TO COUNTER THE USE OF THE ICTS FOR TERRORIST PURPOSES ........ 32

5. GOVERNANCE, DEVELOPMENT & HUMAN RIGHTS ........ 33

5.1 GOVERNANCE ........ 33

5.2 HUMAN RIGHTS ........ 39

5.3 DEVELOPMENT ........ 42

6. CONCLUSIONS ........ 44

ANNEX 1 ........ 47

TABLES ........ 47

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **ARF** | ASEAN Regional Forum |
| **ASEAN** | Association of Southeast Asian Nations |
| **AU** | African Union |
| **CBMs** | Confidence Building Measures |
| **CFSP** | Common Foreign and Security Policy (EU) |
| **CCDCOE** | Cooperative Cyber Defense Centre of Excellence (NATO) |
| **CERT** | Computer Emergency Response Team |
| **CHMS** | Council of Heads of Member States (SCO) |
| **CIS** | Commonwealth of Independent States |
| **CNO** | Computer Network Operations |
| **CoE** | Council of Europe |
| **CSTD** | Committee for Science and Development (UN) |
| **CSTO** | Collective Security Treaty Organisation |
| **DNS** | Domain Name System |
| **ECOSOC** | Economic and Social Council (UN) |
| **ECOWAS** | Economic Community of West African States |
| **EDA** | European Defence Agency |
| **EMC** | European Military Council |
| **EU** | European Union |
| **GCA** | Global Cybersecurity Agenda (ITU) |
| **GCHQ** | Government Communications Headquarters |
| **GGE** | Group of Governmental Experts (UN) |
| **IANA** | Internet Assigned Numbers Authority |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **ICTs** | Information Communications Technologies |
| **IGF** | Internet Governance Forum |
| **ITU** | International Telecommunications Union |
| **LDCs** | Least Developed Countries |
| **MDGs** | Millenium Development Goals |
| **MOU** | Memorandum of Understanding |
| **NATO** | North Atlantic Treaty Organization |
| **NRRCs** | Nuclear Risk Reduction Centers |
| **NSA** | National Security Agency (NSA) |
| **NTIA** | National Telecommunications and Information Administration (US – Department of Commerce) |
| **OAS** | Organization of American States |
| **OECD** | Organisation for Economic Cooperation and Development |
| **OSCE** | Organization for Security and Cooperation in Europe |
| **PC** | Permanent Council (OSCE) |
| **SADC** | Southern African Development Community |
| **SCO** | Shanghai Cooperation Organisation |
| **UN** | United Nations |
| **UNCTTF** | UN Counter Terrorism Implementation Task Force |
| **UNODC** | UN Office on Drugs and Crime |
| **WCIT** | World Conference on International Telecommunications |
| **WSIS** | World Summit on the Information Society |

# ABOUT THE AUTHORS …

**Camino Kavanagh** is currently pursuing a Ph.D. at the Department of War Studies, King's College London, where her focus is on cyberspace and transformation of strategic affairs. She is a Senior Advisor to ICT4 Peace Foundation and to the New York-based National Committee on American Foreign Policy (NCAFP) where she has developed an annual round table series on Cyber Security and US Foreign Policy. Her professional experience includes some fifteen years working in/on conflict and post-conflict settings. She consults regularly for international and government agencies, working between NY, Bamako and London.

**Tim Maurer** is a Research Fellow at New America's Open Technology Institute focusing on cyberspace and international affairs namely cyber-security, Internet Freedom, and Internet governance. In October 2013 and February 2014, he spoke about cyber-warfare at the United Nations and his research has been published by Harvard University, Foreign Policy, CNN, and Slate among others.

**Dr. Eneken Tikk-Ringas** is Senior Fellow for Cyber Security at the International Institute for Strategic Studies (IISS) focusing on conscious exercise of national power in cyberspace and international cyber security related legal and policy issues. She serves as senior expert on cyber security at the Baltic Defence College. Since 2011, Eneken has been advising the Board of the ICT4Peace Foundation on international cyber security.

# ABOUT ICT4PEACE FOUNDATION …

**ICT4Peace** www.ict4peace.org was launched as a result of the UN World Summit on the Information Society (WSIS) in Geneva in 2003 and aims to facilitate improved, effective and sustained communication between governments, 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 Program on Rights and Security in the Cyberspace 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. Sample ICT4Peace publications can be found at: http://ict4peace.org/?p=1076 and include:

- Getting down to business: Realistic goals for the promotion of peace in cyber-space (2011)
- ICT4Peace brief on upcoming Government Expert consultations on Cyber-security (GGE) at the UN in New York (2012)
- An overview of global and regional processes, agendas and instruments (2013)
- What Next? Building Confidence Measures for Cyberspace (2013)
- The Reach of Soft Power in Responding to International Cybersecurity Challenges (2013)

# ACKNOWLEDGEMENTS…

The authors wish to thank Daniel Stauffacher, President of ICT4 Peace Foundation for his comments and for bearing with us as we finalized the report. Particular thanks to Robert Morgus for the excellent research support he provided throughout the drafting process. Robert is a research assistant at New America's Open Technology Institute (OTI) where he works on Internet governance, international cyber security, and human rights online.

The authors would also like to extend special thanks to Ewan Buchanan (UN ODA), Prof. Ron Deibert (Citizen Lab, University of Toronto), James A. Lewis (CSIS), Amb. (ret'd) Paul Meyer (Simon Fraser University), Nemanja Malisevic (formerly OSCE, now Microsoft) and Adam Segal (CFR), for their insightful comments and suggestions on the different drafts of the paper. The research for this paper concluded in March 2014.

# BASELINE REVIEW

## ICT-RELATED PROCESSES & EVENTS

IMPLICATIONS FOR INTERNATIONAL AND REGIONAL SECURITY

(2011-2013)

## 1. BACKGROUND & INTRODUCTION

Over the past five years, states have become increasingly engaged in a series of regional and international policy discussions and debates over 'cyber security.' This engagement stems from a growing sense of insecurity regarding vulnerabilities in computer systems and related technologies, and how they can be exploited for malicious purposes. Vulnerabilities and threats in this environment have been recorded since the 1980s and both state and non-state actors have found innovative ways and means to respond to them.[1] Yet, it was only in the past five to seven years that threats and vulnerabilities were elevated to the seat of high politics and strategy, and placed squarely (oftentimes with exaggerated passion) on national, regional and international security agendas.[2]

The growing interest of states in 'cyber security' has taken place against a background of important shifts in the global strategic environment: the rise of China as a global economic and regional military power; the global financial crisis, the effects of which are still resonating; and an increased assertiveness in international and regional politics on the part of many rising middle income states. The uncertainty in the international environment provoked by these shifts has added to the sense of complexity surrounding discussions and debates on 'cyberspace' and the use of information and communications technologies (ICTs) for attaining political, military or economic advantage. More recently, this interest in greater state involvement was inadvertently stoked by the role ICTs have, and continue to play in the political upheavals in the Middle East and North Africa; the alleged state use of sophisticated malware to achieve foreign policy goals; and Edward Snowden's disclosures on the monitoring and surveillance practices primarily of the U.S. National Security Agency (NSA) and the UK Government Communication Headquarters (GCHQ).

[1] Myriam Dunn-Cavelty, Victor Mauer and Sai Felicia Krishna-Hense (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Ashgate Publications (2007).

[2] Cyber Index: International Security Trends and Analysis (2013), CSIS, IPRSP, UNIDIR. Available at: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Despite a flurry of activity in international and regional fora responding to these concerns, limited progress was made towards reaching consensus on any agenda before 2013. In fact, the outcome of the World Conference on International Telecommunications (WCIT) in Dubai in December of 2012 confirmed deep divisions among states regarding how the Internet should be governed, and a growing overlap between Internet governance and national and international [cyber] security concerns.[3] The outcome of the WCIT conference also confirmed a widening geopolitical divide between states with very different visions of cyberspace – and the Internet in particular: an open, bottom-up ICT environment or 'cyberspace' underpinned by democratic values on the one hand, and a closed, top-down, state-dominated 'information environment' protected by the principles of state sovereignty and non-interference on the other.[4]

Notwithstanding, 2013 witnessed some positive developments with multi-lateral agreements within the framework of the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE) on the applicability of international law and other existing norms and principles to cyberspace, confidence building measures (CBMs) and capacity building measures. Bilateral agreements between Russia and the U.S. on CBMs, and the initiation of other regional and bilateral processes were also promising signs.

At the 2013 Seoul Conference on Cyberspace, the ICT4 Peace Foundation hosted a side-meeting during which strong emphasis was placed on ensuring greater inclusivity with regard to on-going and emerging cyber security-related processes, including with regard to ensuring greater regional participation in related discussions and debate, and greater involvement of civil society, industry and academia (as per the 2013 UN GGE report). ICT4Peace Foundation's related plenary Statement reiterated these views, committing itself to ensuring that information on the different processes reaches a broader geographical audience and establishing means to report these views to government.[5] This report is a first step in this direction.

The report is structured around the following three areas: i) international and regional security (the predominant focus); ii) transnational crime and terrorism; iii) and governance, human rights and development. These areas are obviously interdependent, with developments in one area often impacting another, yet they have traditionally been approached separately through distinct communities of practice and fora. This has been

[3] Danielle Kehl and Tim Maurer (2012), 'WCIT 2012 Has Ended' available at http://www.slate.com/blogs/future_tense/2012/12/14/wcit_2012_has_ended_did_the_u_n_internet_governance_summit_accomplish_anything.html; Danielle Kehl and Tim Maurer (2012) WCIT 2012: A Half-time Analysis of the Summit that Could Shape the Future of the Internet available at http://www.slate.com/blogs/future_tense/2012/12/11/wcit_2012_a_half_time_analysis_of_the_itu_summit_on_internet_governance.html

[4] Tim Maurer and Robert Morgus (forthcoming) CIGI Internet Governance Paper Series

[5] ICT4Peace Side Meeting Report, Seoul Conference on Cyberspace plus Statement, available at: http://ict4peace.org/seoul-conference-on-cyberspace-2013-statement-on-ict4peace-special-session/. See also the UK government's report on its Contribution to the Seoul Conference on Cyberspace, accessible at: https://www.gov.uk/government/publications/uk-contribution-to-the-seoul-conference-on-cyberspace

the case over the past fifteen years; yet more recent developments demonstrate that these policy areas are converging, thus constituting an opportunity for wider ranging agreements on the one hand, and greater risk of misunderstanding and tension on the other. The report will serve as a baseline for future annual reports with this specific one covering the period spanning January 2011 to December 2013. It also highlights some of the core policy events and processes to watch out for in 2014.

Finally, the authors use the terms 'cyberspace' and 'cyber security' with caution throughout the paper, not least because many important challenges regarding definitions remain unresolved.[6] In the West, policy communities tend to use the term 'cyberspace' and 'cyber security'. Other countries, including members of the Shanghai Cooperation Organization (SCO) continue to use the term 'information space' or 'information environment'. The differences in definitions and the confusing manner in which they are sometimes used reflect a significantly different and highly instrumental interpretation of the issues at hand. And while countries are signalling an increased willingness to engage on cyber security issues, real progress will be difficult to achieve if common agreement on definitions and concepts is not reached.

# 2. INTERNATIONAL AND REGIONAL SECURITY

## 2.1 INTERNATIONAL SECURITY

Since the mid-2000s an increasing number of states has placed cyber security or information security on their national security agendas, investing significant resources in developing national capacity to respond to threats and vulnerabilities, and in developing (and fielding) military doctrine and defensive and offensive military capabilities in this field.[7] Reports on how some of these capabilities have been used to attain political objectives within or outside a theatre of war, and the acknowledgement that more countries are developing military cyber strategies and malicious ICT capabilities has compelled states to the table to discuss how such capabilities fall under existing international law and how state uses of these same capabilities might be restrained.

International discussions on the misuse of information communication technologies and the potential implications for international security have been taking place within the UN since 1998 when the Russian Federation tabled a Resolution within the UN General Assembly's First Committee on Disarmament and International Security, reportedly in response to

[6] Keir Giles and William Hagestad (2012), Divided by a common Language: Cyber Definitions in Chinese, Russian and English. Conference paper presented at the 2013 5th International Conference on Cyber Conflict, NATO CCD COE.

[7] Cyber Index: International Security Trends and Analysis (2013), CSIS, IPRSP and UNIDIR. Available at: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

the U.S. military's doctrinal focus on information dominance and information warfare.[8] Three GGEs have since been tasked with discussing information and telecommunications within the context of international security.[9] In 2012, a third GGE was established through Resolution A/Res/66/24, publishing its report in the summer of 2013. Despite very different viewpoints amongst the GGE members, consensus was reached on a range of topics, including norms, confidence and capacity building measures. Moreover, the GGE report confirmed that 'international law, particularly the UN Charter, is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'[10] Agreement was also reached on the applicability of 'state sovereignty and the international norms and principles that flow from sovereignty' to 'state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.'[11] At the same time, the report stressed that efforts to address the security of ICTs would need to go 'hand-in-hand with respect for human rights and fundamental freedoms as set forth in the Universal Declaration of Human Rights and other international instruments.'[12]

[8] See Krutskikh et al (2009) *International Information Security: The Diplomacy of Peace*. Moscow. See in particular essay by Komov (2008), About the Evolution of the Modern American 'Information Operations Doctrine.

[9] Although supported by several states, the general thrust of the Russian Federation's earlier Resolution received limited support. It was not until 2009 when the United States finally decided to join the debate that discussions on norms for state behaviour in cyberspace began to take shape. In 2010, a Group of Governmental Experts (GGE) operating within the framework of the UN GA First Committee held a series of meetings on the 'Creation of a Global Culture of Cybersecurity', agreeing for the first time on a range of measures. Subsequently, in December 2011, the UN General Assembly agreed to establish a new GGE to implement these measures and '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 (...).' See Tim Maurer (2012), Cyber Norm Emergence at the UN: An Analysis of the Activities at the UN Regarding Cyber Security. Belfer Centre for Science and International Affairs; and Eneken Tikk-Ringas (2012), Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012. ICT4 Peace.

[10] Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98) Section III Recommendations on norms, rules and principles of responsible behaviour by States (para.19), available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E

[11] Ibid (para.20)

[12] Ibid (para. 21) Other points agreed upon included the need to intensify cooperation to respond to criminal or terrorist use of ICTs (including harmonization of legislation and collaboration between law enforcement and prosecutorial services); and responsible behaviour by states, notably in terms of 'meeting their international obligations regarding internationally wrongful acts attributable to them; not using proxies to commit internationally wrongful acts; and ensuring that their territories are not used by non-state actors for unlawful use of ICTs.' In its Sections IV and V, the Report also tables a range of *confidence building measures* to 'promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception;' and *capacity building measures* aimed at 'improv[ing] the security of critical ICT infrastructure; develop[ing] technical skill and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridg[ing] the divide in the security of ICTs and their use.' Progress in securing ICTs, including through capacity building the report suggests, would also contribute to the achievement of Millennium Development Goal 8, aimed at 'developing a global partnership for development.' Important to note also that the GGE Report acknowledged the importance of non-state actors – particularly the private sector, academia and civil society – in supporting the implementation of the recommendations of the GGE

The consensus views expressed in the 2013 UN GGE report are a significant development not least in light of difficulties encountered in the previous GGEs (particularly the first one in which no consensus was reached) and in other processes. For example, in September 2011, a group of countries led by the Russian Federation and the People's Republic of China had circulated an 'International Code of Conduct for Information Security' for consideration at the 66th session of the UN General Assembly, arguing inter alia that the increasing militarization of the Internet [by Western nations] propelled the decision to propose the Code.[13] The document received strong backing from the Shanghai Cooperation Organization (SCO), which described it as the 'first relatively comprehensive document proposing international rules on information and network security,' arguing that the language of the document is similar to that of the Universal Declaration on Human Rights in that it aims to build a 'peaceful, secure, open and cooperative Internet space.'[14] China, Russia and the other SCO members had continuously refuted the position of mainly Western countries that the existing laws of armed conflict applied to the 'information environment' and thus proposed the Code as an alternative. Russia brought this position further when it released its 'concept for a Convention on International Information Security' at the second International Meeting of High-Ranking Officials Responsible for Security Matters in Yekaterinburg, Russia in 2011,[15] and engaged in high-level meetings with a range of countries on the merits of the concept, which apparently received the support of some 52 countries.

Both the Code of Conduct and the draft Convention include voluntary provisions banning the use of the Internet for military purposes and for the overthrow of regimes in other countries, again with the unspoken aim of countering the threat of Western cultural influence and military superiority vis-à-vis information communication technologies. Adoption of the texts would assure that individual countries would assume their own sovereign roles with respect to cyberspace policy; and while provisions on freedom of expression and access to information are included in both documents, so are follow-on caveats that render these rights contingent on national security concerns. Indeed, and as noted by Russian information security expert Andrey Krutskikh, 'ensuring information security must not suppress freedom; exercise of freedom must not jeopardize national security and sovereignty.'[16] The SCO's 2009 Agreement on Information Security shares similar provisions, as do several of the agreements shaping high-level ICT strategy and policy in the countries of the Commonwealth of Independent States (CIS). High-visibility

[13] The Code of Conduct was proposed by the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan (A/66/359)

[14] China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations, Ministry of Foreign Affairs of the People's Republic of China, accessible at: http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm See also: C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) Proceedings of the 4th International Conference on Cyber Conflict, 2012. NATO CCD COE Publications

[15] See Concept of a Convention on International Information Security, 28/11/2011 at: http://rusemb.org.uk/policycontact/52

[16] Remarks by Russian MFA representative A.Krutskikh at London Cyber Conference, Nov. 2011.

incidents such as Stuxnet and the important role social media played in the political upheavals in the Arab region reinforced this narrative.

Notwithstanding, the June 2013 GGE Report does mark a shift in the positions of some countries. This shift was reaffirmed by G8 foreign ministers (including Russia) during the 2013 UK Presidency who confirmed 'international law is relevant in the digital world as it is off-line,' and stressed 'the need to take steps to promote transparency and confidence building measures in order to reduce the risk of misperceptions between states.'[17] The assertion of the relevance of international law to cyberspace in the GGE Report was a key objective of the U.S. and other Western states, and has been viewed as a 'gain.' China and Russia achieved a similar 'gain' with the acceptance of the applicability of the principle of sovereignty in the GGE report. Yet, these 'gains' were '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.'[18]

Following a proposal tabled by the Russian Federation in December 2013, a new GGE will be established in 2014 and the group will be increased from the current fifteen to twenty members to broaden representation from the global south.[19] The goal is to continue discussions on the issues that were agreed upon in the 2013 report.[20] Key questions moving forward include agreeing on acceptable state behaviour under the existing international norms. In addition, there is still no international agreement as to what constitutes the use of force in cyberspace. Determining what constitutes an armed attack in cyberspace as well as when to use cyber capabilities in self defence (as per Art. 51 of the UN Charter), will be a complex exercise, in particular determining how the principles of necessity and proportionality apply. Conversely, it is important to note the growing consensus among experts of the limited likelihood that any armed conflict will be solely 'cyber;' rather

[17] https://www.gov.uk/government/news/g8-foreign-ministers-meeting-statement

[18] Paul Meyer, (2013), Confidence Building in Cyberspace: UN Experts Agree it Would be Nice. Canada International Council, accessible at: http://opencanada.org/features/the-think-tank/comments/confidence-building-in-cyberspace/

[19] Member of the new GGE will represent the following countries: P5 + Antigua & Barbados, Belarus, Brazil, Colombia, Egypt, Estonia, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Pakistan, RoK and Spain. The Chair has yet to be confirmed.

[20] Russia tabled a Resolution during this year's UNGA session calling for the establishment of a new GGE in 2014 to continue discussions on these issues. Member states have agreed to this proposal and discussions are on-going to determine when exactly this might happen and what the composition will be, whether 15 members as is generally the case, or an expanded group of 20.

these capabilities will be used in an existing armed conflict to achieve military and political 'effect' and therefore the issue should be explored from that perspective.[21]

It is also likely that the reports of U.S. and UK electronic monitoring and surveillance practices will impact the work of the next GGE. Until relatively recently, issues pertaining to economic and political espionage were largely dealt with on a bilateral level, yet, more recently, the UN General Assembly was used as a platform for responding to issues of concern in this area, while there are increasing overlaps between the ICT-related issues being tabled in the different General Assembly Committees. Following reports that the NSA actively spied on the Brazil and German heads of state, President Roussef of Brazil gave a scathing speech at the opening of the 2013 plenary session of the UN General Assembly in New York.[22] The speech was followed by the co-sponsoring of a Resolution by both countries in the UN General Assembly's Third (Human Rights) Committee on 'The Right to Privacy in the Digital Age' which was adopted without a vote on 18 December 2013,[23] and the hosting of the NetMundial Conference (on which more below) in Sao Paolo in April 2014.

## OTHER

In 2007, the International Telecommunications Union (ITU) adopted a Global Cyber Security Agenda (GCA) and has since used that as a framework for engaging with member states on a range of cyber security-related challenges.[24]

[21] Also worthy of note is that the debate over cyberspace and international security has advanced alongside a broader debate on the applicability of humanitarian law to the use of technologies – particularly Unmanned Aerial Vehicles (UAVs) - in conflict. It is likely that the latter discussion will be placed on the agenda of the next UN General Assembly, although it is unclear how this agenda will relate to the on-going discussion on Information and Telecommunications in the Context of International Security. Efforts by Pakistan to include the use of UAVs on the agenda of the UN Human Rights Council (within the framework of the Council's counterterrorism work) has already created a stir, particularly the U.S. decision to boycott the discussion on the grounds that the Human Rights Council is not the right forum for such a discussion. See NCAFP Roundtable Proceedings, Cybersecurity, U.S. Foreign Policy, and a Changing Landscape and more recently, UNHRC Not Right Forum to Talk about Drones: US on Pakistan's Draft, 21 March 2014. First Post. Available at: www.firstpost.com/world/unhrc

[22] Statement by H.E, Dilma Roussef, President of the Federative Republic of Brazil at the Opening of the General Debate of the 68th Session of the United Nations General Assembly, New York, 24 September 2013. http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

[23] Interestingly, at the same time, the G77 + China introduced a draft Resolution (A/C.2/68/L.40) in the UN General Assembly's Second Committee (Economic and Finance) on ICT for development including language on 'the unauthorised practice of illegal interception' calling for reports by the UN Secretary-General on these practices. This language was removed from the final version of the Resolution (A/68/167) adopted on 18 December 2013, most likely due to opposition and the fact that the issue had already been attended to in the Resolution co-sponsored by Brazil and Germany in the Third Committee. The Resolution can be accessed here: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=http://www.un.org/depts/dhl/resguide/r68_en.shtml&Lang=E

[24] ITU's Global Cybersecurity Agenda (GCA) was adopted by ITU member states in 2007. It focuses on legal measures, technical and procedural measures, organizational structures capacity building, and international cooperation.

Earlier in 2003, the World Summit on Information Society (WSIS) (discussed in more detail in Section 5 below) Declaration of Principles included emphasis on different security issues, including 'building confidence and security in the use of ICTs.'[25] The latter were captured in the accompanying Geneva Plan of Action.[26] In 2005, under the WSIS Tunis Agreement, governments also committed to using ICTs to promote peace and prevent conflict.[27] In 2013, a review process of WSIS, including the security-related sections of the Geneva and Tunis Declaration of Principles, Plan of Action and Commitment, was initiated under the ITU and the UN General Assembly.

In addition to formal multi-lateral processes, in November 2011, the UK government launched a conference series which has since become an annual event. The 'London Conference on Cyberspace' was launched with the intention of bringing in a broader group of stakeholders – particularly like-minded countries – into the broad range of policy discussions and debates that had emerged around cyberspace, particularly cyber security. Since the London meeting, which the UK government used to table a set of Principles for Cyberspace,[28] the Conference has been hosted by the Hungarian (2012) and Republic of Korea (2013) governments. The outcome of the latter conference – the 'Seoul Conference on Cyberspace' - was captured in a document entitled 'Framework for an Open and Secure Cyberspace.'[29] Although many perceive it to be primarily focused on cyber security, the Conference series agenda has broadened its scope, raising questions about its interaction with other fora, namely those focusing on Internet governance.

## 2.2 REGIONAL SECURITY

Parallel to the work of the UN GGE at the international level, states have also been discussing cyber security concerns in regional fora.[30] Some of these processes have

[25] See 'Building the Information Society: A Global Challenge in the New Millennium.' Specifically para. B5 - Building Confidence and Security in the Use of ICTs, specifically paragraphs 35-37 relating to building a trust framework; preventing the use of ICTs for purposes inconsistent with the objectives of maintaining international stability and security; and dealing with spam at the appropriate national and international levels. http://www.itu.int/wsis/docs/geneva/official/dop.html

[26] See Geneva Plan of Action, Action Line C5 (12) on Building Confidence and Security in the Use of ICTs http://www.itu.int/wsis/docs/geneva/official/poa.html

[27] Para. 36, Tunis Commitment: '**We value** the potential of ICTs to promote peace and to prevent conflict which, *inter alia,* negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction.' http://www.itu.int/wsis/docs2/tunis/off/7.html Para. 36 was introduced to the diplomatic negotiations in 2004 by the Swiss and Tunisian Governments for its adoption as part of the WSIS Tunis Commitment in 2005. The ICT4Peace Foundation (www.ict4peace.org) was subsequently established in spring 2006 to raise awareness about the Tunis Commitment and promote its practical realization in all stages of crisis management.

[28] See Footnote no. 111 below.

[29] Information on the Seoul Conference on Cyberspace is available here: http://www.seoulcyber2013.kr/en/about/meeting.html

[30] See ICT4 Peace Report and Matrix on the status of CBMs (updated February 2014) at: http://ict4peace.org/what-next-building-confidence-measures-for-the-cyberspace/

produced positive results, providing a degree of optimism that states may be willing to cooperate and exercise some form of strategic restraint in their uses of ICTs to achieve political ends.

## 2.2.1. ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE)

For example, in December 2013, the Permanent Council (PC) of the Organization for Security and Co-operation in Europe (OSCE) adopted PC Decision 1106 on the 'Initial Set of OSCE CBMs to Reduce the Risks of Conflict Stemming from the Use of ICTs.'[31] Overall, this initial set of CBMs focuses on a number of important transparency measures, which will allow for exchanges of information and communication on several levels.

It includes, *inter alia*, voluntary commitments to share national views on various aspects of national and transnational threats to and in the use of ICTs; to facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs; to conduct consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity; and to share information on measures that have been taken to ensure an open, interoperable, secure, and reliable Internet.[32] The agreement by the OSCE participating States to adopt this initial set of CBMs is particularly noteworthy given the failure of previous attempts to reach consensus. Also worthy of note is the fact that from the outset, the OSCE CBMs were intended to feed into related processes underway in other regional and international entities – such as, the UN GGE or the ASEAN Regional Forum (ARF).

At the same time however, the CBMs agreed upon in December 2013 still remain modest in their scope, and implementation will be difficult to track, not least because of the overall voluntary nature of the agreed CBMs. The latter reflects the fact that no notification or observation measures were included in the agreement. While, on the whole, this initial set of CBMs can and should be understood as an expression of goodwill among the OSCE participating States – and, as such is one of the most positive developments to have occurred in the thematic area over the past years – much work remains to be done.

## 2.2.2. NORTH ATLANTIC TREATY ORGANISATION (NATO)

The North Atlantic Treaty Organization (NATO) has also placed significant focus on cyberspace and cyber security through the operational level integration of 'cyber

[31] OSCE 'Initial Set of OSCE Confidence Building Measures to Reduce the Risk of Conflicts Stemming from the Use of Information Communications Technologies.' PC.DEC/1106 of 3 December 2013. Available at: http://www.osce.org/pc/109168?download=true

[32] http://www.osce.org/pc/109168

defence' into its Defence Planning Process (NDPP), a 'crucial tool providing a framework within which national and Alliance defence planning activities can be harmonized.'[33] Cyber defence has been on the agenda of almost all NATO summits since 2002 and the topic continues to receive high levels of political attention. The different capabilities and national approaches to cyber security among the 28 member states, however, constitute an obstacle to practical allied cyber defence.

The 2012 Chicago Summit emphasized the need for NATO to forge partnerships with the UN, EU, OSCE and partners. In this context, NATO will facilitate the development of strong national cyber defence capabilities within its member states by setting out the capabilities that are needed at the national level, organizing and supporting communication, training, education and exercises, sharing information and best practices and promoting joint capability development processes and projects.[34]

Following the 2007 incidents in Estonia, NATO has also actively pursued efforts to strengthen cyber defence by concluding Memorandums of Understanding (MOU) with a number of states on cyber defence cooperation and coordination. It is expected that similar MOUs will be signed with all NATO Member States by the time the annual NATO Summit takes place in Wales in September 2014. The MOU template will also be adapted in accordance with a new policy that will be tabled for approval at the Wales Summit.[35] Meanwhile, NATO's efforts with partner countries comprise a series of multinational pilot campaigns and expert staff talks on cyber defence with Ukraine. In 2014, NATO will host a series of meetings on cyber security-related CBMs and norms.

In 2013, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), an independent think tank accredited by NATO, released the 'Tallinn Manual on the International Law Applicable to Cyberspace.' Written at the invitation of the CCD COE by 20 legal scholars and practitioners, the Tallinn Manual explores the applicability of international humanitarian law and the doctrines of *jus ad bellum* to cyber conflicts, and offers a range of definitions, including the definition of the much disputed term 'cyber attack.' The expert group rejected any characterisation of cyberspace as a distinct domain subject to a discrete body of law. At the same time however, the exercise demonstrated the enormous challenge of interpreting international law norms in the cyber context.

[33] G8 Foreign Ministers' Meeting Statement – Section on Transnational Challenges and Opportunities: https://www.gov.uk/government/news/g8-foreign-ministers-meeting-statement

[34] At the end of October 2013, NCIA announced NATO Computer Incident Response Capability's (NCIRC) Full Operational Capability (FOC), a major milestone in continuing efforts to consolidate NATO's own network defences. The work on updating and upgrading NATO's cyber defence capabilities will continue, with primary focus on protecting the Alliance's own networks and assisting the Allies with bringing their cyber defence capabilities to a higher level. (REF.) Therefore, NCIRC FOC is not seen as a goal but a long-term commitment and a process. While NATO will not, in the foreseeable future, develop offensive capabilities, Allied Command Operations (ACO) is active in the field of cyber operations. (REF.) Cyber defence is integrated into operational planning and the conduct of operations on the basis of a comprehensive approach and as a combination of threat factors (energy, terrorism, cyber) and response mechanisms (NATO, nations, partners). (REF.) In 2012 the Combined Comprehensive Operations and Management Centre (CCOMC) was opened with a Cyber Defence Cell (CDC) incorporated.

[35] Communication with NATO representative 10/03/2014

A core example in this regard was the difficulty encountered by the group in crafting a consensus understanding of how international law's definition of 'attacks' applies to cyber operations.[36] The group also discovered that 'applying international law principles to cyberspace raises just as many controversies that attend their application on land, at sea, or in the air' - the latter was exemplified in the debate over 'war-sustaining' military operations.[37] While there are legal and political arguments against some of the applications of international law proposed by the group of experts,[38] the Tallinn Manual has, however, advanced the discussion of how international law might apply in and to cyberspace.

### 2.2.3. EUROPEAN UNION

In February 2013, the European Union adopted a cyber security strategy, which focuses principally on ensuring an open Internet, responding more effectively to cybercrime and protecting critical infrastructure.[39] As noted in a recent study, other initiatives within the regional organisation's Common Foreign and Security Policy (CFSP) pillar are less developed, although the region's 2008 Security Strategy included 'cyber threats' as a new category of risks to European Security.[40] The European Defence Agency (EDA) and the EU Military Council (EMC) have been working on different aspects of computer network operations (CNO) since 2008 and a series of research exercises in the field of common defence and seminars have since been held on cyber security and implications for European CFSP with EU military authorities pushing for the development of a common CNO doctrine since 2009.[41] However, as noted these efforts have been stymied by the 'relatively weak wider institutional framework of common EU command and control capabilities' which will undermine EU efforts to build common cyber defence capabilities, 'even within the relatively limited areas of 'operational CNO' that have already been explored within the EU Battlegroup framework.' Responding to serious cyber incidents has until now been the domain of the Council Security Committee (INFOSEC) – 'a high-powered but secretive body that mostly concerns itself with Information Assurance issues.'[42]

[36] Michael N. Schmitt (2012), 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.' Harvard Journal of International Law. (December 2012) Vol. 54 (online)

[37] Ibid.

[38] Oliver Kessler and Wouter Werner (2013), 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare.' Leiden Journal of International Law, Volume 26, Issue 04, December 2013, pp 793-810; and Dieter Fleck (2013), 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual,' Journal of Conflict and Security Law, (Summer 2013) 18 (2): 331-351.

[39] Cyber Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 07-2-2013 JOIN(2013) 1 final.

[40] Alexander Klimburg and Heli Tirmaa-Klaar (2011), Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Action within the EU. Directorate-General for External Policies of the Union- Policy Department, EXPO/B/SEDE/FWC/2009-01/LOT6/09 PE 433.828 APRIL 2011

[41] Ibid.

[42] Ibid.

Despite Information Assurance being identified as a critical area 'that directly impacts the existential security of the EU institutions' it does not have a CFSP mandate and therefore does not inform the CFSP-relevant bodies, even when there has been a probable state-sponsored cyber attack on EU institutions, something which has reportedly happened quite frequently in recent years at least.[43]

## 2.2.4. ASEAN REGIONAL FORUM

Meanwhile, the ASEAN Regional Forum (ARF), in its broader efforts on terrorism and transnational crime, has become a regional platform in Asia for discussion among states on international cyber security issues. A March 2012 workshop focused on proxy actors or 'groups and individuals, who on behalf of a state, take malicious cyber actions against the governments, the private sector and citizens of other states.'[44] Another workshop in September that same year on confidence building measures focused *inter alia,* on 'whether there is a lack of a cyber security legal framework' and how to build norms that reflect unacceptable action by states.[45]

The ARF platform has also been used to discuss the merits of the Code of Conduct tabled by China and Russia.[46] In October 2013 Beijing co-hosted the first ARF workshop on cyber security with Malaysia entitled 'Measures to Enhance Cyber Security—Legal and Cultural Aspects'[47] and throughout the year, the ARF served as a platform for bilateral discussions with China and Japan as well as the U.S. on cyber security confidence building measures (CBMs).[48] Due to the pressing nature of the issues, a second ARF workshop was held in March 2014 – this time co-hosted by Australia and Malaysia in Kuala Lumpur, and purposefully more 'action-oriented' towards reaching common ground on specific cyber security-related confidence building measures for the Asia-Pacific region.[49] Three core outcomes of the Kuala Lumpur CBM workshop include: i) identifying appropriate points of contact, where they exist, and agreeing to sustain them over the coming months and years; ii) establishing clear requirements for baselines of domestic cyber coordination and technical capabilities across ASEAN states; and iii) ensuring that future iterations of the [CBMs] process maintain the trust-building format of the table top exercises conducted at theworkshop.[50]

[43] Ibid.

[44] Co-Chairs' Summary Report ARF Workshop on Proxy Actors in Cyberspace. Hoi An City, Vietnam. 15/03/2012

[45] Co-Chairs' Summary Report of the ARF Seminar on Confidence Building Measures in Cyberspace. Seoul, South Korea. 12/09/2012. Point 8

[46] Ibid. Points 19 and 23

[47] For a commentary on the Beijing ARF workshop, see: http://www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/

[48] http://csis.org/files/attachments/130723_jimlewis_testimony_v2.pdf

[49] For an overview of the outcome of the second ARF workshop on cybersecurity see: http://www.aspistrategist.org.au/cyber-confidence-building-in-the-asia-pacific-three-big-take-aways-from-the-arf/

[50] Ibid.

## 2.2.5. SHANGHAI COOPERATION ORGANISATION (SCO), COLLECTIVE SECURITY TREATY ORGANISATION (CSTO) AND COMMONWEALTH OF INDEPENDENT STATES (CIS)

Additional regional developments include the aforementioned measures – the Code of Conduct and Concept for an International Convention on Information Security - tabled by the Shanghai Cooperation Organization (SCO), the Collective Security Treaty Organisation (CSTO) and the Commonwealth of Independent States (CIS). The attachment of member states to the principles underpinning both documents has remained strong. For example, at a meeting in Beijing in 2012, the SCO Council of the Heads of Member States (CHMS) reaffirmed its commitment to state sovereignty and non-interference, calling for the promotion of a 'peaceful, secure and open information space.' The CHMS also committed to continue promoting the Code of Conduct under the auspices of the United Nations. More recently in September 2013, the SCO CHMS closed its annual meeting with the Bishkek Declaration in which SCO members reaffirmed their commitment to the aforementioned principles 'on the basis of respect for national sovereignty and non-interference in the internal affairs of other countries.'[51]

Different processes relating to international security and Internet governance in the coming 18 months will be key to determining how a balance will be struck between these principles, which thrust the state to the forefront of discussions on cyber security and cyberspace; and other principles aimed at protecting citizens and ensuring the free flow of data within national borders.

Other measures adopted by the CSTO and CIS are particularly focused on responding to threats posed by the terrorist and criminal use of ICTs.

## 2.2.6. ORGANISATION OF AMERICAN STATES (OAS)

Since the early 2000s cyber security has featured on the OAS working agenda. Indeed, the region was the first to develop a strategy to counter threats to cyber security.[52] Yet, as will be discussed in the next section, this focus has centred mainly on ensuring a common framework for dealing with cybercrime and other forms of organized crime, ensuring that states have the relevant capacity to respond to system vulnerabilities, and ensuring that state responses are aligned with OAS efforts to strengthen democratic governance and the regional human rights architecture.

More recently though, countries in the region have been developing military doctrine in certain areas such as communications, electronic and information warfare, framed within national defence strategies. For example, in its 2008 National Defence Strategy, the government of Brazil introduced guidelines for reorganizing the armed forces and for

[51] Council of the Heads of State of SCO Member States. Bishkek Declaration, Bishkek, Kyrgyzstan, 13/09/2013

[52] AG / RES. 2004 (XXXIV-O/04)

adapting the defence industry to ensure domestic provision of needed technologies for the navy, army and air force, identifying 'cybernetics' as a strategic sector for national defence, and establishing a 'Cyber Warfare Communication Centre.'[53] Argentina's armed forces have developed 'joint military doctrine for communications and electronic warfare,' and since 2009 Colombia has been pushing to develop 'a joint doctrine to govern military and police [defensive and offensive] operations in cyberspace.'[54] Notwithstanding, neither the OAS nor any of the sub-regional groupings in Latin America and the Caribbean appear to have developed a common strategic narrative with regard to common defence against cyber security challenges reflecting more pressing concerns in the region[55] and perhaps also the waning influence of the US with regard to exerting its authority and shaping outcomes within the region.[56]

## 2.2.7. AFRICAN UNION

Similarly, the African Union (AU) response to cyber security threats and vulnerabilities has not been expressed in terms of requiring the development of a military response capacity involving the region's armed forces. Beyond the inherent capacity issues the region's armed forces face, the regional body's main common security focus (and that of the region's sub-regional bodies) remains peacekeeping and responding to extremism, and will most likely remain so for the coming period. However, cybercrime has been identified as a core concern and as discussed in the subsequent section, efforts are underway to develop a common cyber security strategy for the region.

Circulated for comments in 2012, the draft convention – currently entitled 'Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa' - was to be adopted at this year's annual AU Summit in Addis in January. The stated objective of the Convention is to 'propose a credible framework for cyber security in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime.' The 'stakes and challenges' the Convention is aimed at responding to include the digital and cultural heritage of individuals, organisations and nations; the survival and sovereignty of states; achieving a level of technological security to prevent or control technological and informational risks; building an information society that respects values, protects rights and freedoms, and protects and guarantees the security of the property of persons, organisations and nations;

[53] Lewis and Timlin (2011).

[54] Ibid.

[55] Although multi-dimensional security was identified as a top priority by the current OAS Secretary-General, this priority is centered on 'the serious public security crisis generated by trafficking in drugs, arms and persons; money laundering and organized crime.' Other priorities of the organization include strengthening democratic governance, enhancing the regional human rights system; and striking a better balance between democracy building and integral development. See Peter J. Meyer (2014), Organisation of American States: Background and Issues for Congress. Congressional Research Service, 7-5700

[56] Ibid.

and contributing to the 'knowledge economy,' guaranteeing equal access to information while stimulating the creation of authentic knowledge.[57]

Formal adoption of the Convention has has however been postponed due to technical delays and a range of concerns that have been raised regarding privacy, freedom of expression, legislative overkill, and the suggestion that too much power was being placed in the hands of judges.[58] It is expected that the draft Convention will be adopted either in July 2014 or January 2015. Meanwhile, African participation in broader international processes regarding cyber security (for example, the new UN GGE in which two African countries will participate) remains limited.

See Table 1: International & Regional Security in Annex 1 below.

# 3. BILATERAL EFFORTS IN THE FIELD OF INTERNATIONAL AND REGIONAL SECURITY

At the bilateral level, several track 1, 1.5 and track 2 dialogues have been taking place between states and other relevant stakeholders on international and regional cyber security issues. These initiatives are aimed largely at building better understanding, trust and confidence between the parties and establishing joint mechanisms to avoid escalation to armed conflict. Track 1 policy dialogues include the processes between China and the U.S. within the framework of their on-going strategic dialogue, as well as between China and the UK, China and Germany, and China and Europe; between Germany and the U.S., and Germany and India; between Russia and India, and Russia and Brazil. On its part, the U.S. is engaged in bilateral discussions with Japan, India, Brazil, Russia, South Africa and South Korea.[59] Meanwhile, ASEAN is hosting discussions with Japan, China and the U.S. (See Figure 1 below).

More specifically, 2013 saw progress on a series of these bilateral dialogues. In June 2013, discussions between China and the U.S. within the framework of the existing Strategic and Economic Dialogue led to agreement on a set of measures symbolizing important first steps toward greater cooperation. The parties agreed to the creation of a bilateral working group to 'enhance mutual trust, reduce mutual suspicion, manage disputes and expand cooperation.' The working group has met twice since it was created in June 2013.[59] In August, Chinese foreign minister Wang Yi told U.S. Secretary of State John Kerry that he saw 'cyberspace' as 'an area where the two countries can increase mutual trust and

[57] AU Draft Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa of 01/09/2012, accessible at: http://au.int/en/sites/default/files/AU%20Convention%20EN.%20(3-9-2012)%20clean_0.pdf

[58] See Gareth van Zyl, Adoption of 'flawed' AU cyber security convention postponed, 21 January 2014; and Kenyan bid to Stop flawed AU cyber security convention. 28 October 2013 at www.itwebafrica.com

[59] www.reuters.com/article/2013/11/06/net-us-usa-china-hacking-idUSBRE9A51AN20131106

cooperation.' This was a significant development after a rise in tensions between both countries around accusations meted out on the topic of cyber industrial espionage, and a statement by the U.S. Congress that the U.S. should view with suspicion the 'continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.'[60] It was also important given the belief amongst Chinese officials that U.S. tech companies are often used as Trojan horses for delivering American political values.[61] In response to some of the information released by Edward Snowden, China's Defence Minister Colonel Yang stated that '[t]he PRISM-gate affair is itself just like a prism that reveals the true face and hypocritical conduct regarding Internet security of the country concerned.'[62] Needless to say, the focus in China on U.S. surveillance practices also stirred domestic concern regarding China's own surveillance practices.[63]

In 2013, the Russian Federation and the U.S. also agreed on the creation of a new working group under the auspices of the Blilateral Presidential Commission (established in 2009 by Presidents Obama and Medvedev), dedicated to 'assessing emerging ICT threats and proposing concrete joint measures to address them.'[64] In addition to the formation of the working group, the Presidents engaged in dialogue in order to 'increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis.'[65] The discussion resulted in the formation of three confidence-building measures (CBMs) agreed upon by the two Heads of State. The first CBM sets up a link between U.S. and Russian Computer Emergency Response Teams (CERTs) in order to 'facilitate the regular exchange of practical technical information on cyber security risks to critical systems.' The second, a measure involving the exchange of notifications, consists of using the established links between Nuclear Risk Reduction Centres (NRRCs) to 'quickly and reliably make inquiries of one another's competent authorities to reduce the possibility of misperception and escalation from ICT security incidents.'[66] The third measure establishes a direct communication line between the White House and Kremlin ensuring that the leaders of both governments are 'prepared to manage the full range of national security

[60] http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

[61] Geekwire, 'China's reaction to NSA surveillance gives Microsoft reason to worry.' 12/07/2013

[62] *The New York Times*, Chinese Defense Ministry Accuses U.S. of Hypocrisy on Spying, 27/06/2013

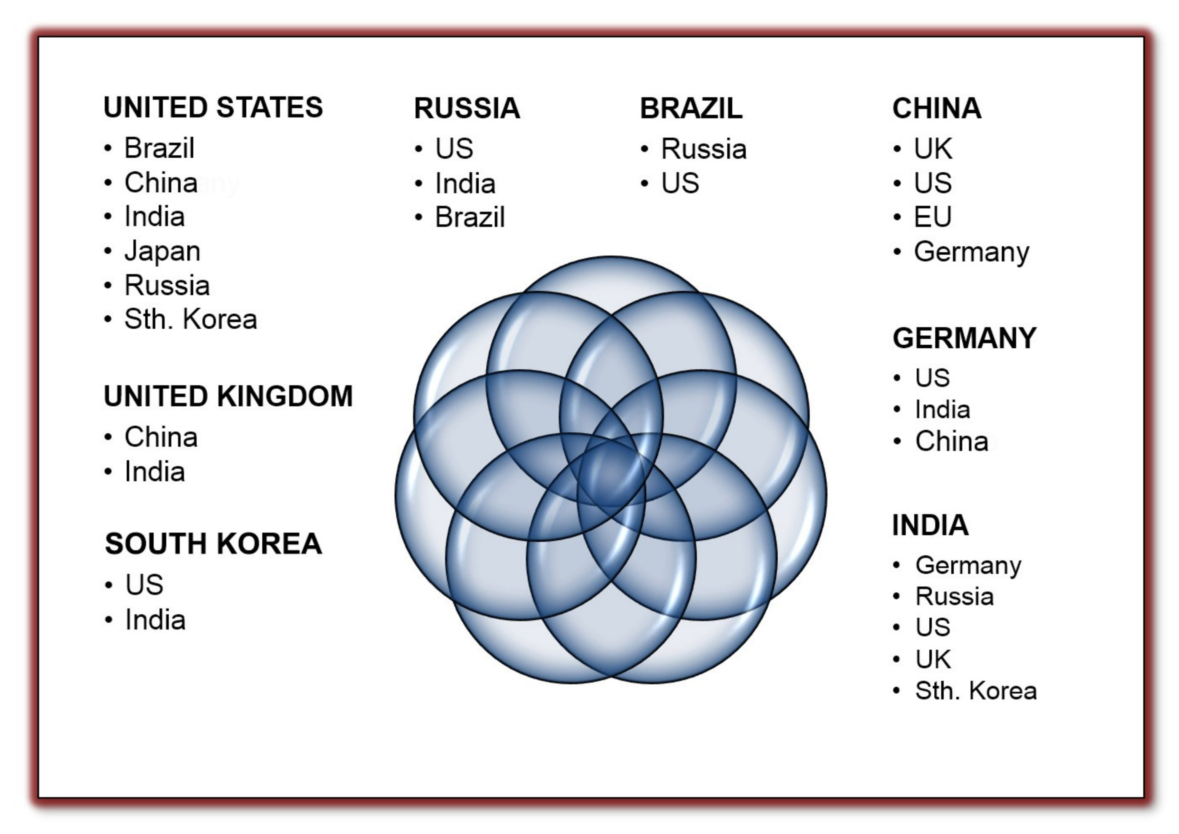
[63] *The New York Times* blog, U.S. Prism, Meet China's Golden Shield, 28/06/2013

[64] http://www.whitehouse.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi. See also: http://www.atlanticcouncil.org/blogs/natosource/us-and-russia-sign-cyber-security-pact Also worthy of mention is the fact that already as far back as 1998, the U.S. and Russia had delivered a joint statement on Common Security Challenges at the Threshold of the 21st Century, which included a specific focus on 'the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution (…), which is a serious challenge to ensuring the future strategic security interests of [the] two countries.' As part of the efforts to resolve these problems, so went the statement, Russia and the U.S. held 'productive discussions within the framework of the Defence Consultative Group on resolving the potential Year 2000 computer problem. Krutskikh et al, 2009, (pp.148-149).

[65] http://www.state.gov/p/eur/cirs/usrussiabilat/c38418.htm

[66] Ibid.

crises' they face.[67] Outside of the working group however, relations have chilled. Following the revelations of NSA surveillance practices, Russian minister Sergei Zheleznyak, called on Russia to 'reclaim its 'digital sovereignty' by introducing legislation that would require all internet traffic in Russia to be hosted on servers in Russia.[68] Strategic concerns regarding Russia's role in the Syria conflict and the more recent crisis in Ukraine will evidently play a role in determining how much progress is made on bilateral discussions regarding the uses of ICTs.



**UNITED STATES**
- Brazil
- China
- India
- Japan
- Russia
- Sth. Korea

**UNITED KINGDOM**
- China
- India

**SOUTH KOREA**
- US
- India

**RUSSIA**
- US
- India
- Brazil

**BRAZIL**
- Russia
- US

**CHINA**
- UK
- US
- EU
- Germany

**GERMANY**
- US
- India
- China

**INDIA**
- Germany
- Russia
- US
- UK
- Sth. Korea

Figure 1. A snapshot of current bilateral ICT-related processes

[67] http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information

[68] Andrei Soldatov and Irina Borogan, Russia's Surveillance State. *World Policy Journal*, Secrecy and Security, Fall 2013

# 4. TRANSNATIONAL CRIME AND TERRORISM

## 4.1 AN INTERNATIONAL CONVENTION ON CYBERCRIME?

Over the past decade, cybercrime has increased alongside the impressive growth in Internet connectivity with both individuals and organized criminal groups exploiting new criminal opportunities for financial gain.

According to a recent study by UNODC, today '[u]pwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information.'[69] Exact cybercrime statistics are not yet sound enough to paint an accurate picture of the extent of cybercrime, although victimization rates appear to suggest a much higher rate of cybercrime victims than for conventional forms of crime.[70]

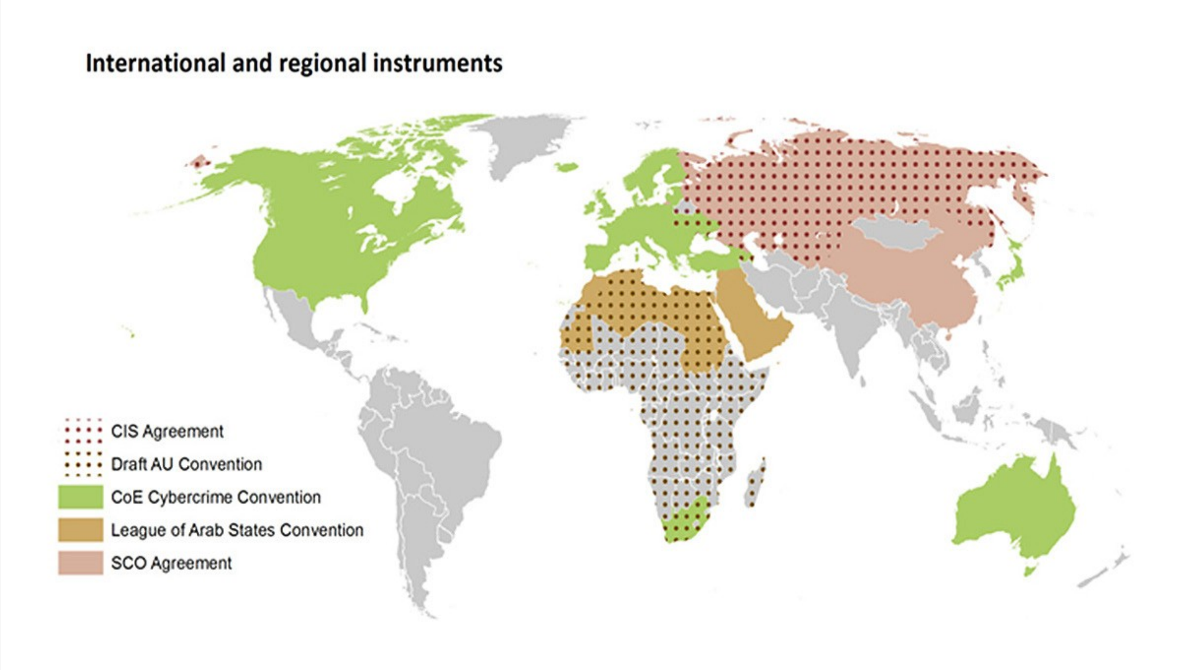

International and regional instruments
CIS Agreement
Draft AU Convention
CoE Cybercrime Convention
League of Arab States Convention
SCO Agreement

Figure 2. Source: UNODC Comprehensive Study on Cybercrime, Draft, February 2013

[69] UNODC Comprehensive Study on Cybercrime, Draft, February 2013. Accessible at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[70] According to UNODC, currently, police-recorded crime statistics do not represent a sound basis for cross-national comparisons, although such statistics are often important for policy making at the national level. Victimization surveys represent a more sound basis for comparison. These demonstrate that individual cybercrime victimization is significantly higher than for 'conventional' crime forms. Victimization rates for online credit card fraud, identity theft, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between 1 and 17 per cent of the online population for 21 countries across the world, compared with typical burglary, robbery and car theft rates of under 5 per cent for these same countries. Cybercrime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen prevention efforts in these countries.

While policy makers and law enforcement officials in some countries have been able to catch up with criminal actors and how the latter take advantage of ICT vulnerabilities for illicit financial gain, important gaps remain.[71] The challenge is even greater for developing or fragile states, where law enforcement capacity is weak, and other pressing priorities take precedence over meeting the high costs of addressing system vulnerabilities and tracking down cyber criminals. Although an increasing number of countries have passed cybercrime legislation, many countries continue to be what have been termed 'jurisdictional voids' from which criminals and intruders can operate with impunity.[72] It is also possible that some jurisdictions, as in the case of other forms of criminal activity, will increasingly seek 'to exploit a permissive attitude to attract business, creating both information safe havens (paralleling offshore tax havens and bank secrecy jurisdictions) that make it difficult for law enforcement to follow information trails and insulated [illicit] cyber-business operations.'[73]

Since the late 2000s discussions on establishing a global framework to respond to the threats posed by transnational cyber crime have centred on whether or not to expand the existing 2001 Council of Europe Convention (the Budapest Convention) on Cybercrime as per the proposal of the EU and the U.S.[74] Japan's ratification of the Convention in July 2012 followed by that of Australia in November that same year was a move in that direction. Yet, several countries remain opposed to accession to the Budapest Convention and have been pushing for the negotiation of a new cybercrime treaty under the auspices of the United Nations. Indications of such positions emerged first in 2008, and were confirmed in 2010 at the UN Congress on Crime Prevention and Criminal Justice held in Brazil when states debated how to tackle what they agreed was a major and growing problem. While Spain (the then holder of the EU presidency) suggested that any international agreement should be an extension of the Budapest Convention, Brazil disagreed, calling for the creation of a new agreement under the banner of the UN that would address regional concerns about cybercrime.[75] Russia itself has rejected a portion of the Convention on the grounds that it 'violates their Constitution by permitting foreign law enforcement agencies to conduct Internet searches inside Russian borders.'[76] Indeed, Article 32 of the Convention relating to

[71] See for example, Melissa Hathaway (2012), Falling Prey to Cybercrime: Implications for Business and the Economy in Nicholas Burns and Jonathon Price (Eds.) *Securing Cyberspace: A New Domain for National Security*. Aspen Institute (February 2012).

[72] Phil Williams (2005), Organized Crime and Cyber-Crime: Implications for Business. Available at: http://www.crime-research.org/library/Cybercrime.htm

[73] Ibid.

[74] The CoE Convention came into force in 2004. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[75] Charles Wild, Stuart Weinstein, Neil Macewan, Neal Geach, Electronic and Mobile Commerce Law: An Analysis of Trade, Finance, Media and Cybercrime in the Digital Age, University of Hertfordshire Press (2011).

[76] Gorman, (2010) cited in Tim Maurer (2011), Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding CyberSecurity, Harvard Kenney School, Belfer Center for Science and International Affairs.

'[t]rans-border access to stored computer data with consent or where publicly available' remains one of its most hotly disputed provisions.[77]

While discussions on whether to draft a new international cybercrime treaty remain the focus of many diplomatic efforts, the question remains whether a new treaty in this area is really necessary, especially given the number of regional conventions on cybercrime already in place or currently being drafted. For example, and as noted earlier, an African Union (AU) Convention on cyber security is currently being finalized and includes a strong emphasis on cybercrime. The increase in cybercrime and the reported costs it is having on sub-Saharan African countries[78] and the 'dire need of innovative criminal policy strategies that embody states, societal and technical responses to create a credible legal climate for cyber security' raised the spectre for the drafting of the convention. A draft was prepared in 2012 and since then a range of workshops and consultations have taken place across the continent via sub-regional bodies such as the Economic Community of West African States (ECOWAS) and the Southern African Development Community (SADC). Despite critics of the draft who have raised concerns regarding privacy protection, supporters of the AU draft Convention stress that it 'tries to address some of the legal loopholes that are exploited in the West.'[79] As noted, it is expected that the draft will be formally adopted in July 2014 or January 2015.

Other regional instruments used as a basis for framing or harmonizing national legislation and mechanisms for cross-border cooperation in the area of cybercrime include the CIS Agreement, the League of Arab States Convention and the SCO Agreement (see Figure 2 above). Meanwhile, political statements and declarations by groups of countries such as the BRICS (Brazil, Russia, India, China, South Africa) have also included strong references to cooperation with regard to cybercrime.[80]

Notwithstanding, signatories of the Budapest Convention continue their advocacy to expand membership to a broader number of states, and today the Budapest Convention reportedly remains the 'most used multilateral instrument for the development of cybercrime

[77] UNODC Comprehensive Study on Cybercrime, Draft, February 2013. New York. Available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[78] It is well known that Cameroon, Ghana, Nigeria and South Africa have become core hubs for cyber criminal activity, particularly fraud yet citizens across sub-Saharan Africa are also falling victim to cyber crime. For example, according to the Norton cybercrime report for 2012, South Africa hosts the third-highest number of cyber crime victims in the world. In addition, the South African Cyber Crime threat Barometer 2012/2013 put the total cost of cybercrime in South Africa between January 2011 and August 2012 at R 2.65 billion. Gareth van Zyl, 'Kenyan bid to Stop flawed AU cyber security convention,' 28 October 2013, available at: www.itwebafrica.com

[79] See blog article: 'The African Union's Cybercrime Convention,' available at: http://i.playgod.org/page/4/

[80] See Draft BRICS Resolution: International Cooperation to Combat Cybercrime submitted to the Commission on Crime Prevention and Criminal Justice, Twenty-second session, Vienna, 22-26 April 2013: Item 7 of the provisional agenda - World crime trends and emerging issues and responses in the field of crime prevention and criminal justice, published by United Nations documents issued on 10-April-13.

legislation.'[81] In November 2013, the Council of Europe launched a new 3-year project – GLACY – aimed at supporting countries with the implementation of the Budapest Convention through the engagement of decision makers to harmonize legislation, train judiciaries, enhance law enforcement capabilities, increase information sharing and international cooperation, and assess progress of implementation.[82] Earlier, the Commonwealth Heads of State also approved an Initiative on Cybercrime bringing Commonwealth members closer to the basic tenets of the Budapest Convention.

Despite the political issues that have delayed an agreement on the most appropriate instrument to respond to transnational cybercrime, both traditional and new forms of international cooperation in criminal matters such as extradition, mutual legal assistance treaties (MLAT), mutual recognition of foreign judgments and informal police-to-police cooperation, or cooperation between police and technology companies have evolved. Indeed, as noted by UNODC, the use of traditional forms of cooperation – particularly MLAT – 'predominates for obtaining extra-territorial evidence in cybercrime cases' with a large number of states falling back on traditional bilateral instruments, and a much smaller number using multilateral instruments.[83] The fact, however, that investigators increasingly access extraterritorial data – either unknowingly or knowingly - during evidence gathering, 'without the consent of the State where the data is physically situated,' is likely to continue to create tensions between states.[84]

## 4.2 OTHER CYBERCRIME-RELATED MEASURES, PROCESSES & DEVELOPMENTS

In 2010, the UN Security Council for the first time formally recognized the threat of cybercrime and other forms of transnational organized crime to international security in a Presidential Statement.[85] And as mentioned in Section 2, in 2013 agreement was reached within the framework of the UNGGE to intensify cooperation to respond to criminal or terrorist use of ICTs (including harmonization of legislation and collaboration between law enforcement and prosecutorial services); while other bodies such as the G8 have focused on the importance of international capacity building efforts to strengthen, *inter alia,* the fight against cybercrime.

[81] Ibid. At the time of writing, the total number of signatures of the Budapest Convention is eleven. The number of ratifications is 42. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

[82] See: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/GLACY/GLACY_en.asp

[83] The UNODC survey report notes that according to responses received, almost 60 per cent of requests use bilateral instruments as the legal basis. Multilateral instruments are used in 20 per cent of cases.

[84] UNODC, Comprehensive Study on Cybercrime: Draft – February 2013. New York. Available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[85] S/PRST/2010/4

More specifically, in 2010, the UN General Assembly adopted three core Resolutions: A/RES/64/211 of March 2010 on the Creation of a Global Culture of Cyber Security; A/RES/64/179 of March 2010 providing a mandate to strengthen United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity in the area of cybercrime; and A/RES/65/230 of December 2010 in which it convened an *intergovernmental expert group* on international responses to cybercrime to which UNODC would act as the Secretariat (see below). In 2012, UNODC established the intergovernmental expert group to conduct the comprehensive study, the objective of which was to develop a 'greater understanding of the threat of cybercrime' and provide 'technical assistance and training to States to improve national legislation and build capacity to deal with cybercrime.'[86] The study highlighted six key findings: fragmentation at the international level; a reliance on traditional means of formal international cooperation; the issue of attribution; a disharmony of national legal frameworks; a lack of law enforcement and criminal justice capacity – especially in developing countries; and weak cybercrime prevention approaches.[87] It builds on related work by the United Nations Crime Prevention and Criminal Justice Programme and the UN Crime Commission.[88] In 2011, ECOSOC's Crime Commission adopted additional Resolutions related to cybercrime: RES 2011/35 on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime; and RES 2011/33 on the Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children.

For several years, the ITU has focused on strengthening the capacity of developing countries to respond to cybercrime within its broader cyber security strategy – the ITU Global Cybersecurity Agenda (GSA). An integral part of its response is focused on harmonising national legislation and policies at the regional and sub-regional levels, including in collaboration with the EU. Also in 2011, the ITU and UNODC signed an MOU to collaborate globally on supporting member states mitigate the risks posed by cybercrime (…) and ensuring secure use of information and communication technologies.[89]

[86] A/RES/65/230

[87] Globally, less than half of the survey respondents perceive their existing criminal and procedural law to be sufficient in cyber-space. The report found that 87 countries have signed a binding cybercrime instrument through the African Union (AU), the Commonwealth of Independent States (CIS), the Council of Europe (CoE), the League of Arab States (Arab League), and/or the Shanghai Cooperation Organization (SCO). In terms of criminalization, it was reported that 13 of 14 widely accepted concepts of cybercrime are criminalized, with SPAM being the one largely non-criminalized facet. Among these concepts, Illegal access, Illegal interception, Illegal interference, and Computer misuse tools are generally recognized as cyber-specific with the others falling under general offences. With regards to police and investigation capacity, 'over 90 per cent of the countries that responded to the questionnaire have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence.' The report does note that these efforts put forth in developing countries are under-resourced and suffer from capacity shortages. On issues of international cooperation, over 70 percent of respondents reported formal cooperation. As noted, about 60 percent of formal cooperation comes in the form of bilateral agreements, with multilateral instruments used 20 percent of the time. UNODC, Comprehensive Study on Cybercrime: Draft – February 2013.

[88] A/RES/64/179 of March 2010

[89] See http://www.itu.int/en/ITU-D/Cybersecurity/Pages/UNODC.aspx

As noted in the previous section, since the early 2000s, the OAS has focused on strengthening measures within the region to counter threats such as cybercrime and the criminal use of ICTs. The latter is of particular concern given how drug cartels operating in the region have used ICTs and related capabilities to circumvent law enforcement, foment terror, and launder illicit monies since the 1990s. In Mexico, for example, the Zeta drug cartel established an independent communications network from the U.S. border down into Guatemala,[90] allowing them to both avoid surveillance and monitor military and law enforcement counter-narcotics activity. Also in Mexico, in late 2011, several bloggers working out of Nuevo Laredo were violently killed by members of drug cartels who berated them *post-facto* for monitoring and participating in online discussions about the drug situation in Mexico and for tipping off authorities about cartel activities. Victims were beheaded or disembowelled, and messages warning others against similar online activities were left on their body parts.[91] Students in the U.S. covering similar activities also received threats.[92] Mexican bloggers and journalists fear that such attacks will prevent people from using the Internet to circulate information on what is happening in different parts of the country, a particularly serious concern given the fact that organised crime has already silenced traditional media.[93] Mexican and regional authorities have been striving to enhance cooperative mechanisms to respond to these kinds of threats which go beyond traditional law enforcement.

Regarding trans-border cybercrime, two core outcomes of OAS efforts include the establishment of the Inter-American Portal and Working Group on Cyber Crime. These were the result of a process of Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA) 'aimed at strengthening hemispheric cooperation in the investigation and prosecution of [cyber] crimes.' The Portal was created with the aim of facilitating and streamlining cooperation and information exchange among government experts from OAS member states with responsibilities in the area of cybercrime or in international cooperation for its investigation and prosecution. The Working Group - established by the REMJA in 1999 – serves as the principal hemispheric forum to strengthen international cooperation in the prevention, investigation and prosecution of cybercrime; facilitate the exchange of information and experiences among its members; and make necessary recommendations to enhance and strengthen cooperation among the OAS member states and with international organizations and mechanisms.[94]

The OSCE has also included cybercrime as a strategic priority in its area of responsibility and is supporting policing organizations in member states to respond to cybercrime-

[90] On how criminal groups use ICT capabilities to circumvent law enforcement see: Camino Kavanagh (ed.), (2013), Getting Smart and Scaling Up: Responding to the Impact of Organised Crime on Governance in Developing Countries. NYU Center on International Cooperation (p.23-24).

[91] *The Houston Chronicle,* Gang Sends Message with Blogger Beheading, 11 November 2011.

[92] *The Economist,* 'The Spider and the Web: The Fog of War Descends on Cyberspace,' 24 November 2011. In 2010 alone, five newspapers admitted in print that due to the risks to their reporters, they would stop covering sensitive drug-war stories. http://www.economist.com/node/21530146

[93] Ibid.

[94] OAS Department of Legal Cooperation: http://www.oas.org/juridico/english/cyber.htm

related threats through capacity-building and related means.[95] In January 2012, it created a new Transnational Threats Department within which the Strategic Police Matters Unit aims to 'increase capacities of law enforcement agencies to effectively address threats posed by criminal activity… including cybercrime.'[96] The aforementioned OSCE PC Decision of December 2013 on CBMs (PC.DEC/1106) also included reference to the terrorist or criminal use of ICTs, specifically the encouragements of states to establish 'modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs.'[97]

At the operational level, in 2013, the European Commission established a European Cyber Crime (E3) Centre at EUROPOL in The Hague. The Centre serves as the focal point in the EU's response to cybercrime, supporting EU member states and institutions 'in building operational and analytical capacity for investigations and cooperation with international partners.'[98] It is specifically mandated to tackle the following areas of cybercrime: crimes committed by organized groups to generate large criminal profits such as online fraud; crimes that cause serious harm to the victim such as online child sexual exploitation; and crimes that affect critical infrastructure and information systems in the European Union.[99]

The G8 High Tech Crime Group, active since 1997, has also played an important role in signalling emerging challenges relating to crime and the Internet as well as other forms of digital crimes and in developing basic operating principles and mechanisms such as the Computer Forensic Principles and 24/7 Network of Contact Points. In 2013, the G8 formally committed to strengthening and expanding the Roma/Lyon High Tech Crime Sub Group (HTCSG) to and the work of the 24/7 Network.[100] In 2014, INTERPOL is set to establish a global cybercrime centre – the Global Complex for Innovation (IGCI) - in Singapore. The new centre will be 'a cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships.'[101]

Other technical assistance and capacity building initiatives include Microsoft's new Cybercrime Centre (Seattle, U.S.), aimed at supporting public-private partnerships in this area,[102] as well as Oxford University's Global Cyber Security Capacity Centre established

[95] James Cockayne and Camino Kavanagh, 'Flying Blind: Political Mission Responses to Transnational Threats.' Thematic Essay, NYU Center on International Cooperation, Annual Review of Special Political Missions (2011). Available at: http://cic.nyu.edu/sites/default/files/political_missions_2011_thematic_kavanagh_cockayne.pdf

[96] OSCE. Annual Report 2012: Building Trust. (pp. 82-83)

[97] See para. 6 of OSCE PC.DEC/1106, 'Initial List of CBMs.' Available at: http://www.osce.org/pc/109168?download=true

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

[99] Ibid.

[100] G8 Foreign Minister's Statement. Available at: https://www.gov.uk/government/news/g8-foreign-ministers-meeting-statement

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

[102] http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/cybercrime-center.aspx

after the London Conference on Cyberspace, which also includes a focus on developing capacity to respond to transnational crime and other cyber security challenges. The World Bank is also supporting the establishment of a Centre of Excellence in Seoul, Korea to bolster the region's efforts in responding to a range of cyber security challenges, including cybercrime.

## 4.3 INTERNATIONAL EFFORTS TO COUNTER THE USE OF THE ICTS FOR TERRORIST PURPOSES

Since the terrorist attacks in the U.S. on 11th September 2001, and as global connectivity has increased and social networking sites have proliferated in multiple languages, terrorist groups have become more sophisticated in their use of the Internet. In the wake of 9/11, extremist groups came under increasing pressure to go underground, finding in the Internet a perfect channel through which it could continue communications while reaching out to a larger audience, and as a means to seek finance for its activities.[103] A UN study noted that between 1998 and 2006, the number of Al Qaeda websites had grown from 12 to approximately 2,600.[104] The same study cited other groups such as Al Qaeda in Iraq, Laskhar e-Taiba, Chechen mujahideen, and Palestinian extremist groups as also using the Internet for a variety of purposes.[105]

In 2006 UN member states pledged to 'coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet' and to 'use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard.'[106] However, as noted in a 2009 Report of the UN Counter Terrorism Implementation Task Force (UNCTTF) Working Group on Countering the Use of the Internet for Terrorist Purposes there is no single integrated approach to address the issue.[107] The report did not focus on the subject of 'cyberterrorism' per se, noting that 'there is not yet an obvious terrorist threat in this area, it is not obvious that it is a matter for action within the counter-terrorism remit of the United Nations.' However, it did note that if a more concrete threat of terrorist cyber attacks materializes in future, 'it might be a more appropriate and longer-term solution to consider a new international counter-terrorism instrument against terrorist attacks on critical infrastructure in general.' If this

[103] Report of the UN Working Group on the use of the Internet for Terrorist Purposes (2009). Available here: http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf A follow up report developed with UNODC was released in 2012 and is available here: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[104] Fourth Report of the Al Qaeda Monitoring Team pursuant to Resolution 1617 (2005), available at: https://www.un.org/sc/committees/1267/monitoringteam.shtml See also Michael Jacobson (2010), Terrorist Financing and the Internet, Studies in Conflict & Terrorism Vol. 33, Iss. 4, 2010

[105] Ibid.

[106] Global Counter-Terrorism Strategy (2006). Accessible at: http://www.un.org/en/sc/ctc/action.html

[107] UNCTITF (2009), Countering the Use of the Internet for Terrorist Purposes. New York, available at: http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_internet_wg_2009_report.pdf

were the case, the definition of critical infrastructure might need to be updated (perhaps by protocol to the treaty) 'to include information infrastructure.'[108]

This issue has continued to figure strongly in UN Resolutions and on international policy agendas, particularly the concern of 'increased use, in a globalized society, by terrorists of new information and communications technologies, in particular the use of the Internet for terrorist purposes, inter alia, recruitment and incitement, as well as for the financing, training, planning and preparation of their activities.'[109]

In 2012, in collaboration with the UNCTTF, UNODC launched a publication – 'The Use of the Internet for Terrorist Purposes' - highlighting some of the core legislative and prosecutorial challenges member states face in responding to terrorist use of the Internet. Intended as a resource for criminal justice practitioners and as a tool for capacity building, the report also stressed the need for 'enhancement of cooperation between criminal justice systems and the private sector, as well as international cooperation, particularly where the preservation and retention of Internet-related data take place in several jurisdictions.'[110] The UNODC study and subsequent criticism also serve as a good example of the tensions between policies focusing on security and those promoting openness and freedom.[111] Meanwhile, several other ICT and terrorism-related issues - for example, the use of censorship to counter radicalization on the Internet - remain controversial.

See Table 2: Transnational Crime & Terrorism in Annex 1 below.

# 5. GOVERNANCE, DEVELOPMENT & HUMAN RIGHTS

## 5.1 GOVERNANCE

Internet governance has become an increasingly contentious policy issue. As will be discussed below, the topic dominated discussions at the World Summit on Information Society (WSIS) in the early- to mid-2000s and subsequent debates and working groups. Yet, more recently it has become increasingly difficult to separate it from the broader international and regional security-related policy processes, not least since some countries have increasingly come to view Internet governance issues and how they are managed, as

[108] Maurer, Tim. "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-security." Discussion Paper 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

[109] See A/RES/68/187 of 11 February 2014 and all earlier Resolutions on Technical assistance for implementing the international conventions and protocols related to counter-terrorism. Accessible at: http://www.un.org/en/terrorism/resolutions.shtml

[110] UNODC and UNCTITF (2012), The Use of the Internet for Terrorist Purposes. New York, 2012. Available at: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[111] Gallagher, Ryan (2012) 'U.N. Report Reveals International Protocol for Tracking People Online' available at: http://www.slate.com/blogs/future_tense/2012/12/04/u_n_office_on_drugs_and_crime_report_reveals_international_protocol_for.html

core to their national security interests. It is also difficult to separate Internet governance from discussions and debates on development and human rightsconcerns.

At the risk of oversimplification, two different perspectives are at the centre of this debate. One perspective has traditionally viewed the Internet as similar to a 'global commons.'[112] This vision of the Internet is connected to what is often referred to as a bottom-up, multi-stakeholder approach to Internet governance including not only governments but the private sector and civil society, and is underpinned by principles of open trade, democratic governance and respect for human rights, particularly freedom of, and access to information. Countries with a strong history of, or aspirations to liberal democratic political systems tend to share this vision, further supported by civil society and the private sector.

A second set of countries has coalesced around a more top-down, territorial vision of how cyberspace should be governed. This vision is underpinned by the principles of state sovereignty and non-interference. Some states view the free flow of information and freedom of expression, particularly through online social fora, as potential threats to state power. This vision of the Internet holds that changes to its architecture should be implemented through national regulation and policy, as well as state-sponsored technological tinkering. Countries that share this vision are highly distrustful of the existing 'multi-stakeholder model,' not least because they view core functions of Internet governance such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA)[113] as indirectly beholden to the U.S. government via the Department of Commerce on the one hand, and because they view Internet-spurred economic growth as generally weighted in favour of U.S. companies on the other.

More recently, the International Telecommunications Union (ITU) - a specialized agency of the UN has come to be considered by some states to be a more appropriate agency for Internet governance. Autocratic governments tend to share this vision, not least because of the potential political power and disruptive effects of ICTs. For a range of reasons, including non-negligible economic concerns, they also tend to associate Internet governance with national and international security and economic development, in some cases referring to the combination of these issues as information security and the information environment.[114] As the Internet and other ICTs became increasingly central to global economies and their overall strategic value increased, so too did the focus on efforts to bring Internet governance under the auspices of the international bodies.

In 2012, the ITU convened the World Conference on International Telecommunications (WCIT). The main purpose of the meeting was to renegotiate a 1988 treaty called the

[112] U.S. Secretary of State, Hillary Rodham Clinton, Internet Freedom speech, January 2011. Available at: http://secretaryclinton.wordpress.com/2011/02/15/secretary-of-state-hillary-clintons-speech-on-internet-freedom/

[113] For insights into ICANN's mandate see: https://www.icann.org/en/about/welcome and for IANA's mandate see: https://www.iana.org/about

[114] See Giles and Hagestad (2013)

International Telecommunications Regulations (ITRs).[115] The build-up to the meeting attracted significant attention among public and private sectors and Internet rights activists as concerns regarding the future of Internet governance mounted.[116] The conference ended in a diplomatic éclat confirming 'deep splits within the international community and a significant challenge to the status quo of how the Internet is governed.'[117] Usually operating by consensus and without a vote, the conference took an unexpected turn during its final days when the head of the ITU asked governments to vote on a revised treaty, which would include references to the Internet.

The conference record listed some 89 states voting in favour of the proposed revisions to the ITRs with some 50 states opposing it.[118] The latter group included the U.S., most European countries as well as some African and Latin American countries. These positions have not been reconciled and it is expected that tensions among these groups of states regarding Internet governance will continue to mount in the coming period. The 2012 WCIT was the first major political struggle over Internet governance since the two World Summits on the Information Society (WSIS) convened in 2003 and 2005[119] when WSIS became the foundation for what is known as the 'multi-stakeholder' model today.[120]

[115] The International Telecommunications Regulations (ITRs) are an old treaty developed in the 1980s and have been re-negotiated several times since then. They were last negotiated in 1988 and they are essentially put in place to facilitate the exchange of international telecommunications traffic across borders as a way to help interconnect the world in terms of communications. Source: Internet Society

[116] See for example, Robert McDowell, The UN Threat to Internet Freedom, The Wall Street Journal, February 21, 2012, available at: http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html?

[117] In late 2011, first reports started to emerge that WCIT could become the forum for the most contentious international debate over Internet governance since 2005 when the process of the World Summit on the Information Society (WSIS) concluded.

[118] See http://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml

[119] For a detailed timeline of the WSIS process, see: Internet Governance Processes: Visualising the Playing Field developed by by Deborah Brown (Access), Lea Kaspar (Global Partners Digital), and Joana Varon (Center for Technology and Society of the Getulio Vargas Foundation). Availabe at: http://wilkins.law.harvard.edu/events/luncheons/2014-02-04_veni/GPD_A3%20Map%20Flyer_P6_Reprint_Web%20version.pdf

[120] Milton Mueller suggests that while most people believe that the WSIS formally legitimated multistakeholder Internet governance (via the 2003 and 2005 outcome documents), governments actually undermined it 'by assigning different 'roles' to each major stakeholder group and giving themselves the most important and powerful role: the 'policy authority for Internet-related public policy issues.' In short, he notes, 'the foundational documents that came out of WSIS were intended to make state actors pre-eminent in the formulation of global Internet policy, and to exclude all others from a direct role in the making of policy. See Milton Mueller's blog-piece *Revisiting Roles: On the Agenda for Brazil,* of December 18, 2013, available at: http://www.internetgovernance.org/2013/12/18/revisiting-roles-on-the-agenda-for-brazil/ An essay by Ambassador A. Krutskikh of Russia in a book compilation on Information Security, confirms that a core objective of the Russian Federation was achieved with the 'adoption of the provision recognizing the lead role of governments in the WSIS process,' and 'the confirmation of the importance of international law, national legislation and sovereignty in developing the international information society.' A. Krutskikh (2009), Advancement of Russian Initiative to Ensure Information Security (chronicles of the decade), in Krutskikh et al (2009), *International Information Security: The Diplomacy of Peace*, Moscow 2009. Elsewhere Mueller notes that the WSIS outcomes, 'with their calls for 'enhanced cooperation' and the creation of the Internet Governance Forum (IGF), pretended to resolve basic disagreements over how global Internet governance should take place.' Yet, as he notes, subsequent events proved that there really was no consensus. See Milton Mueller blog-piece: *The Brazil Meeting X-Rayed,* January 14, 2014, available at: http://www.internetgovernance.org/2014/01/14/the-brazil-meeting-x-rayed/

A rather broad group of countries that have been referred to as 'swing states'[121] has yet to take a firm position with regard to either perspective. For example, in October 2011, India, tabled a proposal at the UN General Assembly for the establishment of a UN Committee for Internet-related policies (CIRP).[122] The CIRP proposal built on the earlier Geneva Declaration of Principles and the Tunis Agenda of the UN World Summit on the Information Society (WSIS)[123] the outcome of which resulted in the establishment of the Internet Governance Forum (IGF) on the one hand, and 'the process towards enhanced cooperation' on the other.[124] The latter has led to a series of UN Resolutions, Secretary-General reports and consultations, culminating in the 2012 UN General Assembly resolution 'Information and communications technologies for development' (A/Res/67/195), and setting in motion the preparatory process for conducting the 2015 UNGA review of WSIS envisaged in the Tunis phase outcome document of 2005 (para.111).[125] The Resolution invited the Chair of the Committee for Science and Development (CSTD) to establish a working group 'to examine the mandate of WSIS regarding enhanced cooperation through seeking, compiling and reviewing inputs from all Member States and all other stakeholders, and to make recommendations on how to fully implement this mandate.'[126] The working group is to report to the 17th Session of the CSTD in 2014 as an input to the overall review of the outcomes of WSIS.[127] Similar discussions have taken place in the context of the 2011 India, Brazil, South Africa (IBSA) Stakeholder Meeting on the Global Internet, endorsed at the 2011 IBSA Summit in Durban, South Africa.[128]

In 2013, a further Resolution was adopted (A/68/198) aimed at 'finaliz[ing] the modalities for the overall review by the General Assembly of the implementation of the outcomes of the World Summit on the Information Society, in accordance with paragraph 111 of the Tunis Agenda, as early as possible, but no later than the end of March 2014.' The Resolution

[121] See for example, Ebert, Hannes and Tim Maurer (2013) Contested Cyberspace and Rising Powers Vol. 34 Iss. 6 *Third World Quarterly*

[122] For the full text of the proposal see: http://ibnlive.in.com/news/full-text-indias-united-nations-proposal-to-control-the-internet/259971-53.html

[123] For background information on WSIS see Milton L. Mueller, Ruling the Root: Internet Governance and the Taming of Cyberspace (2004), MIT Press; Networks and States: The Global Politics of Internet Governance (2013), MIT Press. See also Wolfgang Kleinwächter and Daniel Stauffacher and (Eds), The World Summit on the Information Society: Moving from the Past into the Future (2005), United Nations Task Force Series. Available at: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=169379&lng=en

[124] The origins of the outcome relating to the 'process towards enhanced cooperation' (with regard to Internet governance), reportedly lies 'in the discussions during the WSIS negotiations on the involvement of other countries in the areas where at present the US government exercises some oversight functions over the institutions that manage the Internet's core infrastructure resources.' No agreement was reached at Tunis on this issue, resulting in the nomination of a Special Advisor for Internet Governance to the UN Secretary-General who conducted a series of consultations over 2006 on 'enhanced cooperation.' The Special Adviser – Nitin Desai - presented the results of his consultations in a report to the Secretary General in 2006. The latest development on the 'enhanced cooperation' process included the UN GA Resolution (A/RES/67/195) of 5 February 2013. For a very useful timeline on the 'enhanced cooperation' outcome of WSIS see: http://linguasynaptica.com/timelines/enhanced-cooperation/

[125] The WSIS Review was formalized in UN GA Resolution A/RES/68/198

[126] UN GA resolution, Information and communications technologies for development (A/Res/67/195) of 5 February 2013

[127] Ibid.

[128] Hannes and Maurer (2013), Contested Cyberspace

also 'invite[d] the President of the General Assembly to appoint two co-facilitators to convene open intergovernmental consultations for that purpose.' Interestingly, while an earlier version of the adopted Resolution regarding the WSIS review (A/C/C.2/68/L.40) had included reference to the role of the ITU and its contribution to WSIS and inviting it to make a similar contribution 'to the overall review summit and its preparatory process' this reference was removed in the final Resolution, perhaps indicating some of the tensions simmering below the surface with regard to how member states might be using the ITU to influence certain outcomes. The ITU plenipotentiary in October-November 2014 and the election of a new ITU Secretary-General as well as the WSIS review will affect Internet governance-related discussions moving forward.

As raised earlier, reports of U.S. and UK monitoring and surveillance practices sent important shockwaves through policy communities, including the Internet governance one. Brazil and Germany combined forces at the UN General Assembly to push through a Resolution in the Third Committee on 'The Right to Privacy in the Digital Age.'[129] Subsequently, Brazil announced a global summit - the Global Multistakeholder Meeting on the Future of Internet Governance – 'NetMundial' - in April 2014. While welcoming this initiative, a speech by U.S. Ambassador Daniel A. Sepulveda in January 2014[130] suggested that the Internet Governance Forum (IGF), which will convene this year in Istanbul, might be a more suitable venue to address these issues 'in the most global and inclusive fashion.'[131] U.S. Ambassador Sepulveda also made reference in his remarks to the High Level Panel on Global Internet Cooperation and Governance Mechanisms established by ICANN in 2013, to study the future of Internet governance.[132] The work of this panel, which runs from December 2013 to December 2014, will reportedly draw on the outcome of the Brazil meeting and that of the Freedom Online Coalition (on which more below), which will be hosted by Estonia in April 2014.[133]

Another response to these combined developments was the 'Montevideo Statement on the Future of Internet Governance' released in Montevideo, Uruguay in October 2013 by the 'leaders of organizations responsible for coordination of the Internet technical

[129] UN GA Resolution 'The Right to Privacy in the Digital Age' A/68/167 of 18 December 2013. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=http://www.un.org/depts/dhl/resguide/r68_en.shtml&Lang=E

[130] Remarks by Ambassador Daniel A. Sepulveda, Deputy Assistant Secretary and U.S. Coordinator for International Communications and Information Policy at a panel discussion on Geopolitics and the Future of Internet Governance, Centre for Strategic and International Studies (CSIS), Washington, DC, January 23, 2014, available at: http://translations.state.gov/st/english/texttrans/2014/01/20140125291640.html#axzz2rWOH3Pso

[131] Ibid.

[132] High Level Panel http://www.icann.org/en/about/planning/strategic-engagement/cooperation-governance-mechanisms. See also IGP blog analysis on the overlaps between the High Level Panel and the Brazil conference on the future of Internet governance: http://www.internetgovernance.org/2013/11/19/booting-up-brazil/

[133] Freedom Online Coalition Conference, Tallinn April 2014. http://www.freedomonline.ee/sites/www.freedomonline.ee/files/docs/FOC%20Tallinn%20concept%20paper%20-%20designed%20ver2_0.pdf

infrastructure globally.'[134] The Montevideo statement is significant in the sense that it 'expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance.'[135] The Montevideo declaration also identified the need for 'ongoing effort to address Internet Governance challenges, and (…) catalyze community-wide efforts towards the evolution of global multi-stakeholder Internet cooperation. Moreover, the group of leaders called for an 'acceleration of the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing.' [136] Subsequently, in November 2013, ICANN established a 'Panel on the Future of Global Internet Cooperation' consisting of government, civil society, the private sector, the technical community and international organisations, which met for the first time in London in December 2013. Meanwhile, in March 2014, the National Telecommunications and Information Administration (NTIA) – the U.S. agency principally responsible for advising the President on telecommunications and information policy issues and representing the U.S. government in ICANN's Governmental Advisory Committee (GAC) - announced its intent 'to transition key Internet domain name functions to the global multi-stakeholder community.'[137] As a first step in this direction, the NTIA has tasked ICANN with convening global stakeholders to develop a proposal to transition the current role played by NTIA in the coordination of the Internet's domain name system (DNS).[138]

2014 and 2015 will be key to understanding the real reach of these different Internet governance-related processes. While the U.S. and like-minded states have been pushing to keep the Internet free from state control, some argue that they have actually 'failed to develop a coherent strategic narrative in which defence and development of the Internet are assured, nor have they proposed an architectural framework to counter the models proposed by Russia, China and others.'[139] The lack of strategic coherence is in part related

[134] See: 'Montevideo Statement on the Future of Internet Cooperation.' Available at: http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm

[135] Ibid.

[136] They also called for 'the transition to IPv6 to remain a top priority globally, stressing that '[i]n particular Internet content providers must serve content with both IPv4 and IPv6 services, in order to be fully reachable on the global Internet.' See: http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm

[137] On September 30, 2009, NTIA, on behalf of the U.S. Department of Commerce, reached agreement with ICANN on an Affirmation of Commitments that completed the transition of the technical coordination of the DNS to a multi-stakeholder, private-sector led model and contains provisions to ensure accountability and transparency in ICANN's decision-making with the goal of protecting the interests of global Internet users, as well as mechanisms to address the security stability, and resiliency of the Internet DNS. http://www.ntia.doc.gov/category/icann

[138] See NTIA press release: NTIA Announces Intent to Transition Key Internet Domain Name Functions, available at: http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

[139] See: Preliminary Report on the Cyber Norms Workshop. Roger Hurwitz (co-chair), with Camino Kavanagh, Tim Maurer and Michael Sechrist (rapporteurs). The workshop was sponsored by the Canada Center for Global Security Studies at the University of Toronto, the Belfer Center for Science and International Affairs at Harvard Kennedy School of Government, Explorations in International Cyber Relations, a project at MIT and Harvard, Microsoft Corporation, and MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL). Available at: http://www.citizenlab.org/cybernorms/preliminary_report.pdf

to the dissonance that exists within and between democratic states on competing 'cyber agendas.' In addition, some argue that the current Internet architecture and institutions are perhaps at the end of their life cycle, since they 'do not sufficiently accommodate the shift in Internet demographics to the East and South; they do not give new actors a seat at the decision-making table; and they are not accommodating the on-going growth wave in mobile and cloud computing.'[140] Also of importance is the growing convergence of Internet governance and international cyber security issues, and the implications of this development for on-going diplomatic processes in both areas.[141]

## 5.2 HUMAN RIGHTS

The protection of human rights – particularly the freedom of expression and of opinion - has figured strongly in discussions and debates surrounding cyberspace. A major milestone was reached when the UN Human Rights Council adopted a Resolution in 2012 'affirm[ing] that the same rights that people have offline must also be protected online.'[142] A series of events led to this affirmation. For example, in May 2011, the G8 adopted the Declaration on Renewed Commitment for Freedom and Democracy.[143] Noting that the Internet poses a 'unique information and education resource,' the Declaration acknowledges its potential as a tool to promote human rights, freedom and democracy while stressing the importance of openness, transparency, and freedom as the essential driving forces behind the success and development of the Internet.[144]

In September 2011 the Council of Europe (CoE) adopted Declarations on Internet Governance Principles and on the Protection of Freedom of Expression and Information and Freedom of Assembly and Association with regard to Internet domain names and name strings in September 2011, as well as a series of related recommendations to member states on the protection and promotion of the universality, integrity and openness of the Internet.[145] Together, the declarations affirmed the Council of Europe's commitment to principles fostering a free and open Internet that should be 'upheld by all member states in the

[140] Ibid.

[141] Forthcoming study by Tim Maurer and Meritt Baer on Stuxnet

[142] UN Human Rights Council, Report of the HR Council in its 21st Session A/HRC/21/12 of 26 August 2013, available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session21/A-HRC-21-2_en.pdf

[143] The principles agreed upon '[include] freedom, respect for privacy and intellectual property, multi stakeholder governance, cyber-security and protection from crime that underpin a strong and flourishing Internet.' G8 Declaration - Renewed Commitment for Freedom and Democracy, G8 Summit of Deauville, May 26-27 2011. Note on criticism of the Declaration - ref. Article 19.

[144] http://www.nato.int/nato_static/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf

[145] The CoE principles focus on i) protection and respect for human rights, democracy and rule of law; ii) assurance of multi-stakeholder governance; iii) responsibilities of states vis-à-vis Internet-related public policy that respects Internet freedoms and the rights of individuals; iv) the global nature of the Internet and objective of universal access; vi) the integrity of the Internet; and vii) decentralized management; viii) open architecture; ix; Network neutrality; and x) cultural and linguistic diversity. Available at: https://wcd.coe.int/ViewDoc.jsp?id=1835773

context of developing national and international Internet-related policies.'[146] Specifically, the Declaration on Internet Governance Principles notes the need for Internet governance arrangements to 'ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with human rights law.'[147] The principles formed the basis of the Council of Europe's Internet Governance Strategy (2012-2015) adopted on 15 March 2012.

In October 2011, UK foreign minister William Hague proposed several cyberspace principles at the London Cyber Security Conference.[148] These principles – intended to supply a 'basis for more cooperation between states, business and organizations' - were reconfirmed at the Budapest (2012) and Seoul (2013) Conferences.[149] The principles are similar to those outlined by the OECD and Council of Europe and were suggested as a 'starting point in efforts to reach a broad agreement about behaviour in cyberspace.'[150] The Hague Declaration on Internet Freedom – a first step towards acting on these principles – was signed by some 15 like-minded states in December 2011.[151] Since the meeting in The Hague, a group of countries established the Freedom Online Coalition, consisting of some 22 members spanning Asia, Africa, Europe, the Americas and the Middle East.[152] Endorsement of support for the principles outlined in the Hague Declaration, notably the core principle that all people enjoy the same human rights online as they do offline, is a first obligatory step towards joining the Coalition.[153] The body's main areas of action include diplomatic coordination to advance Internet freedom; support for civil society; and engagement with the private sector to encourage companies to adopt practices and

[146] Ibid.

[147] Ibid.

[148] The seven principles were presented in foreign Minister William Hague's opening speech as follows: The need for governments to act proportionately in cyberspace and in accordance with international law; The need for everyone to have the ability to access cyberspace, including the skills, technology, confidence and opportunity to do so; The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas; Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and expression; The need to respect individual rights of privacy and to provide proper protection to intellectual property; The need for us all to work together collectively to tackle the threat from criminals acting online; and the promotion of a competitive environment which ensures a fair return on investment in networks, services and content. Available at: https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace

[149] https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace

[150] Ibid.

[151] The Declaration was endorsed by Austria, Canada, the Czech Republic, France, Estonia, Ghana, Ireland, Kenya, the Republic of the Maldives, Mexico, Mongolia, the Netherlands, the United Kingdom, the United States and Sweden. Commitments included i) establishing a coalition for information sharing, including on violations and other measures that undermine freedom of expression and other human rights on the Internet; iii) collaboration to support politically and through project aid, the realization of individuals' rights, particularly in repressive environments; and engagement with other stakeholders; iii) bilateral and international cooperation and diplomacy; and iv) engagement with ICT businesses to encourage against adoption of policy and practices that may undermine Internet freedoms and individual rights.

[152] Participating countries include Austria, Canada, Costa Rica, Czech Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Ireland, Kenya, Latvia, the Republic of Maldives, Mexico, Moldova, Mongolia, the Netherlands, Sweden, Tunisia, the United Kingdom and the United States.

[153] See Freedom Online Coalition Factsheet, U.S. Department of State, 20-11-2011. www.humanrights.gov

policies that respect human rights. In parallel to the Freedom Online Coalition, another informal mechanism – the Digital Defenders Partnership – was also established, marking an 'unprecedented collaboration among government donors to provide emergency support for Internet users who are under threat for peacefully exercising their universal rights through new technologies.'[154]

In December 2011, some 34 OECD countries, plus Egypt adopted the OECD Principles on Internet Policy Making.[155] All of the involved parties – initially including governments, private sector stakeholders and civil society – agreed to follow several basic principles committing to the promotion of a free and open Internet when shaping their own Internet policies.[156] While the OECD states and Egypt adopted the recommendation, civil society representatives announced in late-June 2011 that they would not endorse the document due to concerns over intellectual property protection.[157]

These are all generally positive developments. Yet, as noted earlier, Shanghai Cooperation Organisation (SCO) member states have continued to maintain that while language in some of the documents they have adopted or proposed (e.g. the Code of Conduct) speak to the principle values inherent in the Universal Declaration on Human Rights and other human rights treaties and conventions, they still hold that national security considerations will trump human rights concerns if needed.

As discussed, in 2013, the human rights debate took an unexpected turn as the monitoring and surveillance practices of states became public following the NSA and GCHQ disclosures. Already, many states were engaging in increasingly restrictive behaviour, often invoking legal and market pressures to justify the removal of content from Web hosting and social networking platforms, and by offloading policing activities to Internet Service Providers

[154] Ibid.

[155] The OECD principles include: Promoting and Protecting the Global Free Flow of Information; Promoting the open, distributed and interconnected nature of the Internet; Promoting investment and competition in high speed networks and services; Promoting and enabling the cross-border delivery of services; Encouraging multi-stakeholder cooperation in policy development processes; Fostering voluntarily developed codes of conduct; Developing capacities to bring publicly available, reliable data into the policy making process; Ensuring transparency, fair process and accountability; Strengthening consistency and effectiveness in privacy protection at a global level; Maximizing individual empowerment; Promoting creativity and Innovation; Limiting Intermediary liability; Encouraging cooperation to promote Internet Security; Giving appropriate priority to enforcement efforts. Available at: http://www.oecd.org/dataoecd/40/21/48289796.pdf

[156] The Principles are: i) promote and protect the global free flow of information; ii) promote the open, distributed and interconnected nature of the Internet; iii) promote investment and competition in high speed networks and services; iv) promote and enable the cross-border delivery of services; v) encourage multi-stakeholder co-operation in policy development processes; vi) foster voluntarily developed codes of conduct; vii) develop capacities to bring publicly available, reliable data into the policy-making process; viii) ensure transparency, fair process, and accountability; ix) strengthen consistency and effectiveness in privacy protection and global level; x) maximise individual empowerment; xi) promote creativity and innovation; xii) limit internet intermediary liability; xiii) encourage co-operation to promote Internet security; and xiv) give appropriate priority to enforcement efforts. Available at: http://www.oecd.org/internet/innovation/48289796.pdf

[157] http://www.internetgovernance.org/2011/06/28/civil-society-defects-from-oecd-internet-policy-principles/

(ISPs),[158] with many democratic countries passing 'far-reaching surveillance measures that enable widespread eavesdropping on e-mail, cellular phone and other communications activities by requiring ISPs to retain, and when required, turn over such information to legal authorities.'[159] While these issues certainly began to garner attention in the late-2000s particularly as they became a core focus of the reports of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,[160] the NSA revelations led to a flurry of policy activity, including the Seven Principles to Guide State Surveillance Activity offered by Swedish foreign minister Carl Bildt in a speech at the Seoul Conference in Cyberspace in October 2013;[161] the tabling (and subsequent approval) in December 2013 in the UN General Assembly's Second Committee of the aforementioned UN Resolution on the 'Right to Privacy in the Digital Age' (RES/68/198); and a UN Human Rights Council Report on the Implications of State Surveillance of Communications on the Exercise of the Human Rights to Privacy and Freedom of Opinion and Expression.[162]

## 5.3 DEVELOPMENT

It is difficult to discuss security, governance or human rights issues without linking them to economic and social development, not least since a large part of the world still lives in poverty.[163] For the past two decades, developing countries have repeatedly stressed the need to bridge the digital divide i.e. 'the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard to both their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities. The digital divide reflects various differences among and within countries'[164] Other factors such as quality of Internet connections and related services; and affordability are also considered as important. The major arguments for bridging the digital divide have centred principally on: economic equality, social mobility, democracy and economic growth.[165] In 2000, a specific emphasis on ICTs was included in the Millennium Development Goals (MDGs), with MDG 8 emphasizing

[158] Ronald Deibert, John Palfry, Rafal Rohozinski and Jonathan Zittrain, *Access Contested: Security, Identity and Re- sistance in Asian Cyberspace* (Cambridge, MA: MIT Press, 2012), 31-32. See also Frank La Rue, Annual Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/ HRC/17/27 (Section 3)

[159] Ronald Deibert and Rafal Rohozinski, 'Control and subversion in Russian cyberspace,' in *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), 15-34

[160] For a list of the Reports, see: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx

[161] http://www.regeringen.se/sb/d/17280/a/226590

[162] A/HRC/23/40 accessible at: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/23/40&Lang=E

[163] Human Development Report 2013 http://www.undp.org/content/undp/en/home/librarypage/hdr/human-development-report-2013/

[164] OECD Glossary of Statistical Terms accessible at: http://stats.oecd.org/glossary/detail.asp?ID=4719. See also the OECD publication, Understanding the Digital Divide at http://www.oecd.org/internet/ieconomy/1888451.pdf

[165] See Internet World States: The Digital Divide, ICT and the 50x15 Initiative, available at: http://www.internetworldstats.com/links10.htm

the need to develop a 'global partnership for development.' More specifically, one of the targets of the MDG goal involved states cooperating with the private sector to 'make available the benefits of new technologies, especially information and communications.'[166]

More recently, these discussions have become increasingly enmeshed with other agendas, including cyber security and cybercrime. Middle-income countries such as Brazil face important challenges. While important focus has been placed on ensuring broadband Internet access to the country's low-income population, the government, its business community and Brazil's significant online population continue to suffer huge losses to domestic forms of cybercrime and cyber attacks due in part to delays in passing key legislation balancing both privacy and security concerns.[167] Brazil and its highly qualified tech population could serve as important vectors for capacity building if the country manages to overcome such challenges.

West Africa, a region that hosts 13 of the world's least developed countries (LDCs) and where 14 of the 16 countries in the region are ranked amongst the lowest in human development in the world,[168] is home to some of the biggest cybercrime scamming networks in the world.[169] It is also a region where law enforcement faces enormous challenges in responding to organized crime and extremism, and the sophisticated technologies the latter can avail of to advance their goals.[170] However, until relatively recently development agencies were reluctant to include a focus on cybercrime in their assistance to developing countries, alleging in some instances, that cybercrime does not have a direct impact on the poor.[171] There is evidence however, that this approach is gradually changing.

Since the late 2000s, increasing emphasis has been placed on the importance of building capacity in states that may require assistance in 'addressing the security of their ICTs' to the extent that the latest GGE report dedicated an entire section to the topic. More specifically, the report emphasizes the importance of building capacity across states, particularly developing countries, and lays out a series of capacity building measures for states to consider. Such measures range from supporting bilateral, regional multilateral and international capacity building efforts in a range of targeted areas: reform and

[166] See MDG, Target 8(f), Millennium Development Goals and Beyond 2015, available at: http://www.un.org/millenniumgoals/pdf/Goal_8_fs.pdf

[167] See for example, *Bloomberg*, 'Why are Hackers Flooding into Brazil,' 13 September 2013. Available at: http://www.bloomberg.com/news/2013-09-13/why-are-hackers-flooding-into-brazil-.html; *Forbes*, 'Hackers Stole $ 1Billion in Brazil, the Worst Prepared Nation to Adopt Cloud Technology,' 3 February 2012. Available at: http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation-to-adopt-cloud-technology/

[168] For the list of least developed countries, see: http://www.nationsonline.org/oneworld/least_developed_countries.htm and the 2013 Human Development Report Index, see: http://www.undp.org/content/undp/en/home/librarypage/hdr/human-development-report-2013/

[169] Cote d'Ivoire, Ghana and Nigeria in particular are renowned for identity fraud, credit card theft and all manner of Internet scams.

[170] See Kavanagh *et al*, (2013), Getting Smart and Scaling Up: Responding to the Impact of Organized Crime in Developing Countries. NYU Center on International Cooperation (CIC), available at: http://cic.nyu.edu/content/responding-impact-organized-crime-governance-developing-countries

[171] Interviews conducted in London, May 2013.

harmonization of legislation; countering crime and terrorism and the identification and sharing of good practices; developing and strengthening inter and intra-CERT capacities; exploiting ICTs as a means to help overcome the digital divide and facilitate greater involvement of developing countries in international policy processes; transferring capacity and technology to developing countries for dealing with ICT security incidents; to ensuring a greater involvement of research institutes and academia on ICT-related issues.[172]

The GGE report also emphasized that these measures could contribute not only to securing the use of ICTs but also to the attainment of MDG 8. This emphasis is timely, not least since MDG 8 is considered one of the 'weak' MDGs,[173] with the main determinants of ICTs resting on technological factors (mobile phone and Internet access per 100 inhabitants) and remaining largely disconnected from international cooperation on the one hand, and socio-economic realities on the other.[174]

See Table 3: Governance, Development & Human Rights in Annex 1

# 6. CONCLUSIONS

The past decade has seen a significant increase in state interest and involvement in cyberspace. This interest and involvement is directly linked to growing concerns regarding the malicious uses of ICTs by states and non-state actors alike, and the corresponding impact on national, regional and international security. Reports of state uses of ICT capabilities for broad brush surveillance purposes runs the risk of eroding cooperation and trust between states, while states' failure to uphold core rights and principles through efforts to enforce controls on content is impacting state-society relations. As such concerns have mounted, so too have calls for more responsible state behaviour and calls for reaching agreement on the applicability of existing norms and principles, and on transparency and confidence building measures between states; revisiting existing governance arrangements, and bridging the persistent digital divide between developed and developing countries through targeted capacity building. Although important progress has been made through international and regional processes, significant work remains in order to translate some of the difficult agreements reached in 2013 into concrete and verifiable actions. All of this comes at a time when cooperation and trust is most needed

[172] Ibid. Section V. Recommendations on Capacity Building (para.s 30-33)

[173] Report of the UN System Task Team on the Post 2015 UN Development Agenda. Available at: http://www.un.org/millenniumgoals/pdf/mdg_assessment_Aug.pdf

[174] The core indicators for meeting the ICT-specific target in MDG 8 included (i) Fixed telephone lines per 100 inhabitants; (ii) Mobile cellular subscriptions per 100 inhabitants (iii) Internet users per 100 inhabitants. According to Kenny and Dystra, despite the increase in Internet users and mobile telephones, there is limited empirical evidence to date to show that the Internet and mobile phones have played a uniquely significant role amongst [technology] infrastructures in promoting economic and social development. See Charles Kenny and Sarah Dykstra (2013), The Global Partnership for Development: A Review of MDG 8 and Proposals for the Post-2015 Development Agenda. Background research paper submitted to the High-Level Panel on the Post-2015 Development Agenda. See also Report of the UN System Task Team on the Post 2015 UN Development Agenda.

to deal with the manifold pressures – both existing and emerging - on the international system on the one hand, and national state building efforts – in developing and developed counties alike - on the other.

The next eighteen months will therefore be crucial for determining the direction of each of the processes discussed in this report. As they stand, however, these processes raise more questions than answers. For example:

- Will the new UN GGE manage to agree on *how* the international norms and principles agreed upon in 2013 apply in practice? What will the principle obstacles be in this regard? And how will regional or bilateral processes feed into the GGE process and vice versa?
- What incentives exist for states to restrain their uses of ICTs as a means to attain military and political effect if the international system is already facing serious crises of legitimacy outside of the cyber security realm? Will the confidence building measures agreed upon within the framework of the UN GGE, OSCE and ARF actually build trust and transparency between states or will the processes around them just serve as dilatory mechanisms while states build up their capabilities in an endless (and increasingly dangerous) game of strategic reciprocity in which the malicious use of ICT capabilities as a means to achieve political goals becomes the norm?
- How will recommendations in the 2013 UN GGE Report regarding the importance of involving civil society, the private sector and academia in discussions on international cyber security be implemented in practice?
- Will states reach an agreement on a common framework for dealing with cybercrime and all the complex jurisdictional issues inherent in such an agreement or will the trump card of sovereignty be forever tabled to prevent such an agreement from seeing the light? What incentives can be mustered to avoid such an outcome? Are regional instruments sufficient to ensure cooperation and collaboration in dealing with cybercrime issues? What lessons can be extracted in this regard from global counter-terrorism and anti-money laundering cooperative mechanisms and measures?
- What will be the result of the different processes embarked on to determine the future of Internet governance? Will the outcome of these meetings, largely led by governments, really matter or will market tendencies and consumer preferences outpace government efforts in this area? How will the growing convergence between Internet governance and international cyber security issues be reconciled in on-going processes?
- Will capacity building efforts in the international cyber security field have a positive impact on developing countries as per MDG 8 and the targets of the post-2015 development agenda? How will such progress be measured and assessed? Moreover, how will those providing such capacity building assistance avoid the pitfalls of capacity building efforts in traditional security and development fields?

- And last but not least, how will human rights be protected across all of these agendas?

These and many other questions require serious consideration as each of the processes outlined in this report moves forward. For that however, they require more responsive and responsible states.

# ANNEX 1

## TABLES

## TABLE 1

| | | | | |
|---|---|---|---|---|
| 2013 | **EU**<br>CYB.SEC STRATEGY+ PROPOSAL x a DIRECTIVE<br>(FEB.) | **G8**<br>FOREIGN MINISTERS STATEMENT<br>(APR.) | **UNGA**<br>A/68/98<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC.<br>GGE REPORT (No.2)<br>(JUNE) | **OSCE**<br>PARL. DEC.& RES. on CYB.SEC<br>(JULY) |
| 2012 | **OSCE**<br>PC DEC. 1039<br>DEV. of CBMS to REDUCE RISKS of CONFLICT FROM USE OF ICTs<br>(APRIL) | **OSCE**<br>MC.DEC/4/12<br>EFFORTS TO COUNTER TRANS. THREATS<br>(DEC.) | **AU**<br>AU/CITMC-4/MIN/Decl.(IV)<br>KHARTOUM DECLARATION<br>(ENDORSES DRAFT CONVENTION ON CONFIDENCE AND SECURITY IN CYBERSPACE - STILL PENDING FORMAL ADOPTION) | **UNGA**<br>A/67/167<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC.<br>REPORT of THE SG<br>(JULY) |
| 2011 | **OSCE**<br>PC DEC.991<br>OSCE ROLE In CYBERSEC.<br>(MARCH) | **NATO**<br>ADOPTION of new CYBER DEFENCE POLICY + ACTION PLAN<br>(JUNE) | **UNGA**<br>A/66/152 and A/166/152/Ad.1<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELECOMS IN THE CONTEXT OF INT. SEC. REPORT of THE SG<br>(JULY) | **UNGA**<br>A/66/359<br>(1st COMM)<br>LETTER to UNSG from CH, RU, TAJ, UZB re. INT. CODE OF CONDUCT FOR INFO SEC<br>(SEPT.) |
| 2010 | **AU**<br>ASS/AU/11(XIV)<br>DECLARATION ON ‘INFORMATION COMMUNICATION TECHNOLOGIES IN AFRICA: CHALLENGES AND PROSPECTS FOR DEVELOPMENT’<br>(ENDORSES 2009 DECISION TO DEVELOP A REGIONAL CYB SEC STRATEGY)<br>(FEB.) | **UNGA**<br>A/RES/64/211<br>(2nd COMM)<br>CREATION OF A GLOBAL CULTURE OF CYBERSECURITY<br>(MARCH) | **UNGA**<br>A/65/154<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC. REPORT of THE SG<br>(JULY) | **UNGA**<br>A/65/201<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC.<br>GGE REPORT (No.1)<br>(JULY) |
| 2009 | **SCO**<br>AGREEMENT on COOP in FIELD of INFO.SEC | **AU**<br>EXT. CONFERENCE of AU MINISTERS REQUESTS AU COMMISSION to PREPARE AU CONVENTION ON CYB. SEC<br>OLIVER TAMBO DECLARATION | **UNGA**<br>A/RES/63/139<br>DEV.S IN THE FIELD OF INFO & TELECOMS IN THE CONTEXT OF INT. SEC.<br>On Report of the First Committee (A/63/385)]<br>(SEPT) | **UNGA**<br>A/64/129<br>A/64/129/Ad.1<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC.<br>REPORT of THE SG<br>(JULY/ SEPT.) |
| 2008 | **STO**<br>DEC. of COUNCIL of CSTO on PROG. of ACTION to FORM SYSTEM of INFO SEC. of STATE MEMBERS of the AGREEMENT on COLLECTIVE SEC.<br>(SEPT.) | **CIS**<br>DEC. of HEADS of STATE COOP. in FIELD of INFO SEC _ ACTION PLAN<br>(OCT.) | **NATO**<br>SUMMIT DEC.<br>Art. 47 - ADOPTION of POLICY on CYBER DEFENCE<br>(DEC.) | **UNGA**<br>A/RES/62/17<br>DEV.S IN THE FIELD OF INFO & TELECOMS IN THE CONTEXT OF INT. SEC.<br>On Report of the First Committee (A/62/386)<br>(JAN.) |
| 2007 | **ITU**<br>GLOBAL CYBERSECURITY AGENDA | | | |
| 2006 | **UNGA**<br>A/60/288<br>(NO REF. TO COMM)<br>UN GLOBAL CT STRATEGY - INC. PROV. ON COUNTERING USE OF INTERNET X TERRORIST PURPOSES + OTHER INT. LEGAL INSTRUMENTS | **UNGA**<br>A/61/161<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC<br>(JULY) | **UNGA**<br>A/RES/60/45<br>DEV.S IN THE FIELD OF INFO & TELECOMS IN THE CONTEXT OF INT. SEC.<br>On Report of the First Committee (A/60/452)<br>(JAN.) | **WSIS**<br>TUNIS COMMITMENT<br>WSIS-05/TUNIS/DOC/7-E<br>(PARA. 36 Re. USE OF ICTS to PROMOTE PEACE AND PREVENT CONFLICT)<br>(NOV.) |
| 2004 | **OAS**<br>AG / RES. 2004 (XXXIV-O/04)<br>INTER-AMERICA REG. STRAT. TO COMBAT THREATS to CYB.SEC | **UNGA**<br>A/RES/58/199<br>(2nd COMM.)<br>CRTN. OF A GLOBAL CULTURE OF CYB.SEC + PROT. OF CRIT. INFRAST. | **UNGA**<br>A/RES/59/61<br>DEV.S IN THE FIELD OF INFO & TELECOMS IN THE CONTEXT OF INT. SEC.<br>On Report of the First Commiittee<br>A/59/454<br>(DEC.) | |
| 2003 | **UNGA**<br>A/RES/57/239<br>(2nd COMM.)<br>CRTN. OF A GLOBAL CULTURE OF CYB.SEC | **UNGA**<br>A/RES/53<br>DEV.S IN THE FIELD OF INFO & TELECOMS IN THE CONTEXT OF INT. SEC.<br>On Report of the First Commiittee<br>A/57/505<br>(DEC.) | **WSIS**<br>GENEVA DEC. of PRINCIPLES<br>WSIS-03/GENEVA/DOC/ 4-E<br>(Para. B5 Re. BUILDING CONFIDENCE & SEC. IN THE USE OF ICTS)) and Plan of Action<br>WSIS-03/ENEVA/DOC/5-E (PARA. C5 Re. BUILDING CONFIDENCE & SEC. IN THE USE OF ICTS) | |
| 1998 | **UNGA**<br>A/RES/53/70<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC.<br>Followed by resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 | | | |

## INTERNATIONAL & REGIONAL SECURITY

CORE RESOLUTIONS, DECLARATIONS, AGREEMENTS, DECISIONS & REPORTS

| | | | | |
|---|---|---|---|---|
| **UNGA**<br>A/68/156 and<br>A/68/156/Ad.1<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC.<br>REPORT of THE SG<br>(JULY/ SEPT.) | **UNGA**<br>A/RES/68/243<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC.<br>(REQ. x NEW GGE)<br>(DEC.) | **UNGA**<br>A/RES/68/198<br>(2nd COMM)<br>INFORMATION AND ICTS FOR DEV. WSIS REVIEW<br>(DEC.)<br>(Inc. re. sec. reccs in WSIS 3003 and 2005) | **OSCE!**<br>PC DEC. 1106 INITIAL SET of CBMS to REDUCE RISKS of CONFLICT FROM USE OF ICTs<br>(DEC) | **OSCE**<br>MC.DEC/2/13<br>STRENG. EFFORTS TO COUNTER TRANS. THREATS<br>(DEC.) |
| | | | | |
| | | | | |
| **NATO**<br>MOU w. GOV. of ESTONIA on CYBER DEFENCE | **AU**<br>AU/CITMC/MIN/Decl.(III<br>ABUJA DECLARATION<br>(CONFIRMS RESOLUTION TO DEVELOP A REGIONAL CYB SEC STRATEGY) | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## TABLE 2

| | | | |
|---|---|---|---|
| 2013 | **EU**<br>EST. OF EUR. CYBERCRIME CENTER AT EUROPOL STEMS FROM EU CYB.SEC STRATEGY + PROPOSAL x a DIRECTIVE<br>(FEB.) | **UNODC**<br>COMPREHENSIVE STUDY ON CYBERCRIME<br>(DRAFT-FEB) | **G8**<br>FINAL STATEMENT OF FOREIGN MINISTERS<br>(APR.)<br>(INC. PROVISIONS ON CRIME) |
| 2012 | **UN GA**<br>A/RES/66/178<br>TA FOR IMPLEMENTING THE INT. CONVENTIONS & PROTOCOLS X THE PREVENTION OF TERRORISM (INC. PROVISION RE. USE F INTERNET X TERRORIST PURPOSES)<br>(MARCH) | **UNODC/UNCTTF**<br>REPORT ON USE OF INTERNET FOR TERRORIST PURPOSES | |
| 2011 | **UN ECOSOC**<br>E/RES/2011/35<br>INT.COOPERATION IN THE PREVENTION, INVESTIGATION, PROSECUTION & PUNISHMENT OR ECONOMIC FRAUD AND IDENTITYRELATED CRIME | **UN ECOSOC**<br>E/RES/2011/33<br>PREVENTION, PROTECTION AND INTERNATIONAL COOPERATION AGAINST THE USE OF NEW INFORMATION TECHNOLOGIES TO ABUSE AND/OR EXPLOIT CHILDREN | **UNGA**<br>A/66/359<br>(1st COMM)<br>LETTER to UNSG from CH, RU, TAJ, UZB re. INT. CODE OF CONDUCT FOR INFO.SEC / INC PROVISIONS ON CRIME<br>(SEPT.) |
| 2010 | **UNSC**<br>PRESIDENTIAL STATEMENT S/PRST/2010/4 TRANSNATIONAL THREATS AS THREATS TO INT. PEACE & SEC. (INC. REF. TO CYBERCRIME)<br>(FEB.) | **UNGA**<br>A/64/211<br>(2nd COMM)<br>CREATION OF A GLOBAL CULTURE OF CYBERSECURITY<br>(MARCH) | **UNGA**<br>A/RES/64/179<br>(3RD COMM)<br>STRENGTHENING THE UN'S CRIME PREVENTION + CRIM. JUST. PROG<br>(ESP. TA)<br>(MARCH) |
| 2009 | **SCO**<br>AGREEMENT on COOP in FIELD of INFO.SEC<br>(INC. PROVISIONS ON CT -COUNTER-TERRORISM) | **G8**<br>FINAL STATEMENT of JUST & HOME AFFAIRS MINISTERS<br>(REF. CYBERCRIME) | **AU**<br>COMMENCEMENT OF PROCESS TO DRAFT AU CONVENTION ON CYBERSEC (INC. PROVISIONS ON CRIME)<br>(DRAFT CONVENTION as of JAN. 2013) |
| 2008 | **CSTO**<br>DEC. of COUNCIL of CSTO on PROG.of ACTION to FORM SYSTEM of INFO SEC. of STATE MEMBERS of the AGREEMENT on COLLECTIVE SEC.<br>(INC. PROVISIONS ON CRIME + TERRORISM)<br>(SEPT.) | **CIS**<br>DEC. of HEADS of STATE COOP IN FIELD OF INFO SEC + ACTION PLAN (INC. PROVISIONS ON CRIME + TERRORISM)<br>(OCT.) | |
| 2004 | **CoE**<br>CONVENTION ON CYBERCRIME<br>(BUDAPEST CONVENTION)<br>(ENTERS INTO FORCE) | **OAS**<br>AG / RES. 2004 (XXXIV-O/04)<br>INTER-AMERICA REG. STRAT. TO COMBAT THREATS to CYB.SEC (INC. PROVISIONS ON CYBERCRIME) | **G8**<br>SUB-GROUP ON HIGH TECH CRIME<br>WASHINGTON COMMUNIQUE<br>(OPERATIONAL SINCE 1997) |

## TRANSNATIONAL CRIME & TERRORISM

RELEVANT RESOLUTIONS, DECLARATIONS, AGREEMENTS, DECISIONS & REPORTS

| | | | |
|---|---|---|---|
| **UNGA**<br>A/RES/68/98<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOMS IN THE CONTEXT OF INT. SEC. (*AGREEMENT ON APPLICABILITY OF INT. LAW, SOVEREIGNTY + STATE RESPONSIBILITY TO CYB.SPACE*)<br>GGE REPORT (No.2)<br>(JUNE) | **UN ECOSOC**<br>E/RES/2013/39<br>INT.COOPERATION IN THE PREVENTION, INVESTIGATION, PROSECUTION & PUNISHMENT OR ECONOMIC FRAUD AND IDENTITY-RELATED CRIME<br>(JULY) | **OSCE**<br>PC DEC. 1106 INITIAL SET of CBMS to REDUCE RISKS of CONFLICT FROM USE OF ICTs (INC.REF TO CRIME)<br>(DEC) | **OSCE**<br>MC.DEC/2/13<br>STRENG. EFFORTS TO COUNTER TRANS. THREATS<br>(DEC.) |
| | | | |
| | | | |
| **UNGA**<br>A/RES/65/230<br>REQ. FOR ST. OF INT.GOV. WORKING GROUP ON INT. RESP. TO CYBERCRIME (AS PER SALVADOR DECLARATION)<br>(DEC.) | | | |
| REPORT OF THE UNCTTF ON COUNTERING THE USE OF INTERNET FOR TERRORIST PURPOSES | | | |
| | | | |
| | | | |

## TABLE 3

| | | | | | |
|---|---|---|---|---|---|
| 2013 | **UNGA**<br>A/RES/67/195<br>(2ND COMM.- ICT x Development)<br>ON THE REPORT OF THE 2ND COMM. A/67/3\434<br>(FEB.) | **UNGA**<br>A/68/65-E/2013/11<br>REPORT OF THE SEC-GEN ON PROGRESS MADE IN THE IMPLEMENTATION OF AND FOLLOWUP TO THE OUTCOMES OF THE WSIS AT THE REGIONAL AND INTERNATIONAL LEVELS<br>(MARCH) | **UNGA - ECOSOC/CSTD**<br>E/2013/31-E/CN.16/2013/5<br>REPORT OF THE COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT ON ITS FIFTEENTH SESSION<br>(JUNE) | **UNGA**<br>A/RES/68/98<br>(1st COMM)<br>DEV.S IN THE FIELD OF INFO & TELCOM S IN THE CONTEXT OF INT. SEC. (INC. PROVISIONS ON HR + DEV.)<br>GGE REPORT (No.2)<br>(JUNE) | **SEOUL CONF. ON CYBERSPACE**<br>FRAMEWORK FOR AN OPEN AND SECURE CYBERSPACE<br>(OCT.) |
| 2012 | **UNGA**<br>A/67/65/-E/2012/48<br>(2ND COMM.- ICT x Development)<br>REPORT OF WORKING GROUP ON IMPROVEMENTS TO THE IGF<br>(MARCH) | **UNGA**<br>A/67/66-E/2012/49<br>(2ND COMM.- ICT x Development)<br>REPORT OF THE SEC-GEN ON PROGRESS MADE IN THE IMPLEMENTATION OF AND FOLLOWUP TO THE OUTCOMES OF THE WSIS AT THE REGIONAL AND INTERNATIONAL LEVELS<br>(MARCH) | **UNGA - ECOSOC/CSTD**<br>E/2012/31-E/CN.16/2012/4 (SUPP. 11)<br>REPORT OF THE COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT ON ITS FIFTEENTH SESSION<br>(MAY) | **UNGA**<br>E/RES/2012/5<br>ASSESSMENT OF PROGRESS MADE IN THE IMPLEMENTATION AND FOLLOW UP TO THE OUTCOMES OF WSIS<br>(AUG.) | **UN HR Council**<br>A/HRC/21/12<br>REPORT OF THE HR COUNCIL IN ITS 21ST SESSION<br>(AUG.) |
| 2011 | **UNGA**<br>A/66/64-E/2011/77<br>(2ND COMM.- ICT x Development)<br>REPORT OF THE SEC-GEN ON PROGRESS MADE IN THE IMPLEMENTATION OF AND FOLLOW-UP TO THE OUTCOMES OF THE WSIS AT THE REGIONAL AND INTERNATIONAL LEVELS<br>(MARCH) | **UNGA**<br>A/66/67-E/2011/79<br>(2ND COMM.- ICT x Development)<br>REPORT OF WORKING GROUP ON IMPROVEMENTS TO THE IGF<br>(APRIL) | **UNGA**<br>A/66/77<br>(2ND COMM - ICT X DEVELOPMENT)<br>REPORT OF THE SG ENHANCED COOPERATION ON PUB.POL. ISSUES PERTAINING TO THE INTERNET<br>(MAY) | **G8**<br>DEAUVILLE DECLARATION ON RENEWED COMMITMENT X FREEDOM & DEMOCRACY<br>(MAY) | **OECD**<br>PRINCIPALS ON INTERNET POLICY MAKING<br>(JUNE) |
| 2010 | **UNGA (CSTD)**<br>E/2010/31<br>E/CN.16/2010/5 REPORT OF PANEL ON ENHANCED COOPERATION (MAY) | **UNGA**<br>E/RES/2010/2<br>ASSESSMENT OF THE PROGRESS MADE IN THE IMPLEMENTATION OF AND FOLLOW-UP TO THE OUTCOMES OF WSIS<br>(JULY) | **IGF**<br>VILNIUS<br>(NOV.) | | |
| 2009 | **UNGA**<br>A/RES/63/202<br>(2ND COMM.- ICT x Development)<br>On the Report of the 2nd Committee (A/63/411) adopted by GA in Dec. 2008<br>(JAN.) | **UNGA** (A/64/64-E/2009/10) (2ND COMM)<br>REPORT OF THE SEC-GEN ON PROGRESS MADE IN THE IMPLEMENTATION OF AND FOLLOWUP TO THE OUTCOMES OF THE WSIS AT THE REGIONAL AND INTERNATIONAL LEVELS<br>(MARCH) | **UNGA**<br>(E/2009/92*)<br>(2ND COMM)<br>REPORT of the SEC-GEN onENHANCED COOPERATION ON PUBLIC POLICY ISSUES PERTAINING TO THE INTERNET<br>(JULY) | **IGF**<br>SHARM EL SHEIK<br>(NOV.) | |
| 2008 | **UNGA**<br>(A/63/72-E/2008/48)<br>(2ND COMM.- ICT x Development)<br>REPORT OF THE SEC-GEN ON PROGRESS MADE IN THE IMPLEMENTATION OF AND FOLLOW-UP TO THE OUTCOMES OF THE WSIS AT THE REGIONAL AND INTERNATIONAL LEVELS<br>(APRIL) | **UNGA**<br>(A/63/411)<br>(2ND COMM.- ICT x Development)<br>REQUESTS UN SECRETARYGENERAL SUBMIT TO ECOSOC IN 2009 'A REPORT WHICH MAY CONTAIN RECOMMENDATIONS ON HOW THE PROCESS TOWARDS ENHANCED COOPERATION SHOULD BE PURSUED'.<br>(DEC.) | **IGF**<br>HYDERABAD<br>(DEC.) | | |
| 2007 | **IGF**<br>RIO de JANEIRO | | | | |
| 2006 | **UNGA**<br>A/RES.60/252 WSIS<br>(APRIL) | **IGF**<br>ATHENS | UN Special Advisor to the UNSG REPORT on ENHANCED COOPERATION<br>(APRIL) | | |
| 2005 | **UNGA**<br>(2nd COMM)<br>A/RES/59/220 WSIS<br>(FEB.) | **WSIS**<br>TUNIS AGENDA<br>WSIS-05/TUNIS/DOC/6-E<br>(NOV.) | **WSIS**<br>TUNIS COMMITMENT WSIS-05/TUNIS/DOC/7-E<br>(NOV.) | | |
| 2003 | **UNGA**<br>(2nd COMM)<br>A/RES/57/238 WSIS | **WSIS**<br>GENEVA DEC. of PRINCIPLES WSIS-03/GENEVA/DOC/ 4-E<br>and Plan of Action WSIS-03/ENEVA/DOC/5-E | | | |
| 2002 | **UNGA**<br>(2nd COMM)<br>A/RES/56/183 WSIS | | | | |

# INTERNET GOVERNANCE, HUMAN RIGHTS & DEVELOPMENT

RELEVANT RESOLUTIONS, DECLARATIONS, AGREEMENTS, DECISIONS & REPORTS

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **SEOUL CONF. ON CYBERSPACE**<br>SEVEN PRINCIPLES TO GUIDE STATE SURVEILLANCE/<br>(OCT.) | **IGF**<br>BALI<br>(OCT) | **MONTEVIDEO STATEMENT** on FUTURE OF IG<br>(NOV.) | **UNGA**<br>A/RES/68/198<br>(2nd COMM)<br>INFORMATION AND ICTS FOR DEV. WSIS REVIEW<br>(DEC. adopted JAN. 2014) | **UN HR COUNCIL**<br>A/HRC/23/40<br>REPORT OF SPEC. RAPP. ON IMPLICATIONS OF STATE SURVEILLANCE OF COMMS. ON EXERCISE OF HR TO PRIVACY AND FREEDOM OF OPINION AND EXPRESSION | **UNGA**<br>A/68/167<br>(3rd COMM)<br>On the Report n the report of the Third Committee (A/68/456/Add.2)<br>RIGHT TO PRIVACY IN THE DIGITAL AGE<br>(DEC.) | | |
| **UNGA**<br>A/67/357<br>REPORT OF SPEC. RAPP ON FREEDOM OF EXP.<br>(SEPT.) | **IGF**<br>BAKU<br>(NOV.) | **UNGA**<br>A/67/3\434<br>REPORT OF THE 2ND COMM - ICT X DEVELOPMENT<br>(DEC.) | **WCIT**<br>DUBAI<br>FINAL ACTS<br>(DEC.) | | **CoE**<br>CM(2011)175 final<br>INTERNET GOV. STRATEGY 2012-2015 | | |
| **UNGA**<br>A/66/290<br>REPORT ON FREEDOM OF EXP. THROUGH THE INTERNET<br>(AUG.) | **CoE**<br>DECLARATION ON INTERNET GOV PRINCIPLES<br>(SEPT.) | **CoE**<br>DECLARATION ON PROT. OF FREEDOM OF EXPRESSION & FREEDOM OF ASSEMBLY<br>(SEPT.) | **IGF**<br>NAIROBI<br>SEPT. | **LONDON CONF. on CYBERSPACE**<br>PRINCIPLES X CYBERSPACE<br>(OCT). | **INDIA**<br>PROPOSAL TO THE UNGA ON EST. OF [UN] COMMITTEE FOR INTERNETRELATED POLICIES<br>(OCT.) | **IBSA**<br>TSHWANE DECLARATION (ART.52-55) + OUTCOME OF IBSA MEETING ON GLOBAL INTERNET GOVERNANCE<br>(OCT.) | **HAGUE DECLARATION** on INTERNET FREEDOM<br>(NOV.) |

# ABOUT ICT4PEACE FOUNDATION ...

ICT4Peace www.ict4peace.org was launched as a result of the UN World Summit on the Information Society (WSIS) in Geneva in 2003 and aims to facilitate improved, effective and sustained communication between governments, 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 Program on Rights and Security in the Cyberspace 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. Sample ICT4Peace publications can be found at: http://ict4peace.org/?p=1076 and include:

- Getting down to business: Realistic goals for the promotion of peace in cyber-space (2011)
- ICT4Peace brief on upcoming Government Expert consultations on Cyber-security (GGE) at the UN in New York (2012)
- An overview of global and regional processes, agendas and instruments (2013)
- What Next? Building Confidence Measures for Cyberspace (2013)
- The Reach of Soft Power in Responding to International Cybersecurity Challenges (2013)

ICT for peace
FOUNDATION