CENS WORKSHOP ON CBMS AND NORMS FOR CYBERSECURITY AND THE FUTURE OF INTERNET GOVERNANCE

3 – 4 JULY 2014, SINGAPORE

Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS), Singapore

THE ROLE OF CIVIL SOCIETY IN FURTHERING CONFIDENCE BUILDING MEASURES

Dr. Daniel Stauffacher President, ICT4Peace Foundation
www.ict4peace.org

ICT for peace foundation

The Genesis of ICT4Peace

I am not a “techie”, I am not an ICT specialist, but I have the right and responsibility as a citizen of this world, to understand how the internet and the web is shaping our life and that of our children.

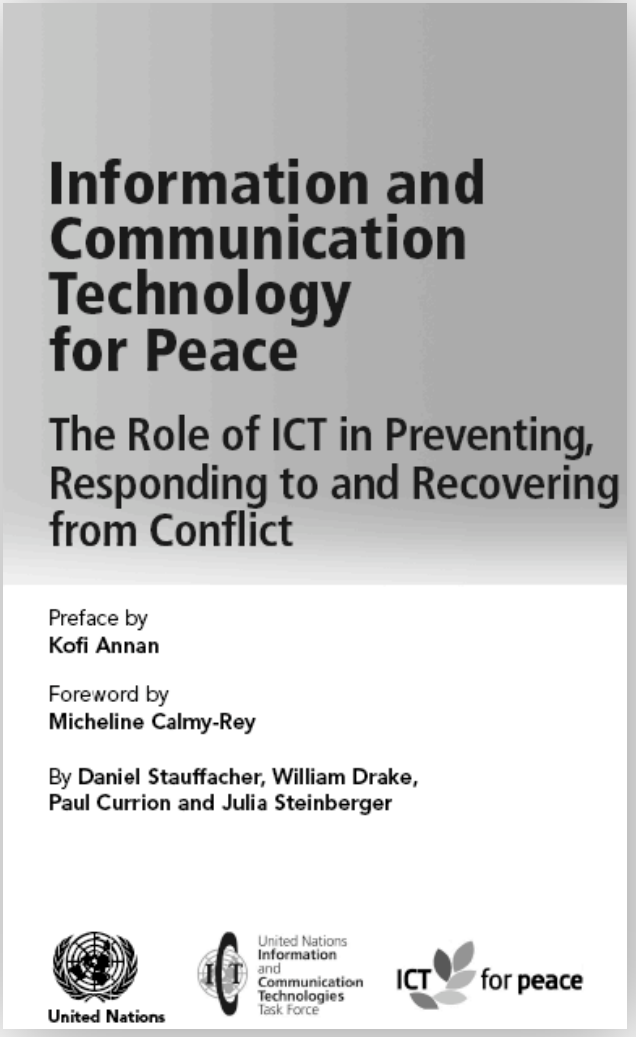
The idea of trying to understand the role of information and communication technologies (ICTs) in promoting and building peace came out of my involvement with the World Summit on the Information Society (WSIS) as a chief representative of Switzerland, the host country of the first phase of the Summit, which was held in 2003 in Geneva.

As the WSIS Geneva Declaration of Principles and Plan of Action emphasized the central role of ICTs in many areas of economic and social development. The risk of a growing 'digital divide', where ICTs could reinforce rather than reduce inequalities, was acknowledged, and recommendations were made in order to turn the digital divide into a digital opportunity for all.

However, development and prosperity can only be achieved if the local situation is peaceful and stable. Peace is a necessary prerequisite to social and economic development. Throughout the world, many regions experiencing conflicts are cut off from development opportunities. Also, in recent years, we have witnessed decades-worth of excellent development work by countries and international organisations destroyed by conflict in a matter of weeks. The return on investing in conflict prevention, or in building lasting peace is indefinitely larger than the investments that are required to reconstruct countries and build peace after conflict.

The
Role of ICTs in
Preventing, Responding
to and Recovering from
Conflict

WSIS Tunis 2005
ICT4Peace/UN ICT Task Force
(http://bit.ly/1bR0yPI)



The UN World Summit on the Information Society (WSIS) in Tunis 2005

•Paragraph 36 of the World Summit on the Information Society (WSIS) Tunis Declaration (2005):

•*"36. 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."* between peoples, communities and stakeholders involved in crisis management, humanitarian aid and peacebuilding.

Report of the UN Secretary-General (A/65/491)
Status of implementation of the information and communications technology strategy for the United Nations Secretariat.

- ***Crisis information management strategy.*** *The Crisis Information Management Strategy is based on the recognition that the United Nations, its Member States, constituent agencies and non-governmental organizations need to improve such information management capacity in the identification, prevention, mitigation, response and recovery of all types of crises, natural as well as man- made. The strategy will leverage and enhance this capacity and provide mechanisms to integrate and share information across the United Nations system.*

- *The Office of Information and Communications Technology (CITO), together with the Office for the Coordination of Humanitarian Affairs (OCHA), the Department of Peacekeeping Operations and the Department of Field Suppor (DPKO and DFS), has worked closely with United Nations organizations such as the Office of the United Nations High Commissioner for Refugees (UNHCR), the United Nations Children's Fund (UNICEF), the United Nations Development Programme (UNDP) and WFP and other entities such as the ICT for Peace Foundation in developing and implementing this strategy. It is envisaged that membership will be expanded to include other United Nations organizations in the near future.*

ICT for peace foundation

Home | About Us | Media | Contact

SEARCH

UPDATES

PUBLICATIONS

FEATURED ARTICLES

EVENTS

LIKE US ON FACEBOOK

FOLLOW US ON TWITTER

New Media: Tools & Techniques for Civilian Crisis Management

14 Jan 2014

Course Description
This course introduces participants to a variety of new ...*more*

Video: What's so Big about Big Data?

14 Jan 2014

Recorded at the 5th Annual International Conference of Crisis Mappers, ...*more*

2013 and ICT4Peace: Year

Getting down to business: Realistic goals for the promotion of peace in cyber-space

See Article by Barbara Weekes et al (2011): "Getting down to Business – Realistic Goals for the Promotion of Peace in the Cyberspace: http://ict4peace.org/getting-down-to-business-realistic-goals-for-the-promotion-of-peace-in-cyber-space/
See list of articles by ICT4Peace on rights and security in the cyberspace: http://ict4peace.org/?p=1076.

WSIS 2003 Geneva Plan of Action
Follow-up towards 2015, MDGs and beyond

Action Line C5. Building confidence and security in the use of ICTs

- **12.** Confidence and security are among the main pillars of the Information Society.
- Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate fora to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.
- Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.
- Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.
- Take appropriate action on spam at national and international levels.
- Encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication.
- Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.
- Share good practices in the field of information security and network security and encourage their use by all parties concerned.

Confidence Building in Cyberspace: Constructive work by UN experts

United Nations A/68/98*

General Assembly

Distr.: General
24 June 2013

Original: English

Sixty-eighth session
Item 94 of the provisional agenda**
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Note by the Secretary-General

OSCE

Organization for Security and Co-operation in Europe
Permanent Council

PC.DEC/1106
3 December 2013

Original: ENGLISH

975th Plenary Meeting
PC Journal No. 975, Agenda item 1

DECISION No. 1106
INITIAL SET OF OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and

ICT4Peace Seoul Statement on Cybersecurity

Report on Ict4Peace Workshop and Statement to Seoul Conference Plenary: http://ict4peace.org/seoul-conference-on-cyberspace-2013-statement-on-ict4peace-special-session/

UN GA THIRD COMMITTEE APPROVES TEXT TITLED 'RIGHT TO PRIVACY IN THE DIGITAL AGE'**

- It calls on states to **review procedures, practices and legislation on communications surveillance and "to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data.**"
- It also asks U.N. human rights chief Navi Pillay to present a report to the U.N. Human Rights Council and the U.N. General Assembly on the protection and promotion of the right to privacy in domestic and extraterritorial surveillance and the interception of digital communications and collection of personal data, including on a mass scale.
- The difficult political and legal questions underlying references to "unlawful interference with privacy" and constraints on "extraterritorial surveillance" will keep lawyers and diplomats busy for months if not years to come.
- At the same time, the challenge of reconciling the occasionally conflicting imperatives of ensuring national security and respecting human rights cannot be ignored by governments or citizens alike. At the multilateral level, the UN will have to begin to address the cyber security issue in a more coherent fashion.
- The General Assembly can ill afford to have two deliberative streams (i.e. the First and Third Committee) acting in ignorance of one another. The airing of declaratory policy at the annual General Assembly sessions should not substitute for purposeful action by states in more operational forums to tackle the pressing problems raised by destabilizing state conducted cyber operations.

(**See also Paul Meyer: http://ict4peace.org/cyber-security-takes-the-un-floor/)

The Cybersecurity Challenge

- Numerous states are pursuing military cyber-capabilities: UNIDIR Cyber Index**: 114** national cyber security programs world-wide, **47** have cyber-security programs that give some role to the armed forces.
- Cyber capabilities are **not limited to great military powers**. They transcend lines of state-centered warfare: **A private** cannot usually obtain, train and use weapons of war. In the electronic world they can.
- The **step from common crime to politically motivated acts**, even **terrorism**, is not far.

Cyber Capabilities and traditional security calculus

- An exclusive, all-out cyber-**war has not happened yet**, but attacks have happened as part of conflicts: 2007 against Estonia, 2008 against Georgia, 2010 against Iran, 2013 against South Korea. In the context of the Syrian war, denial-of-service attacks have been reported.
- Cyber action can also **create real damage in the physical world**. The Stuxnet virus resulted in the destruction of equipment; Destruction of a country' certain critical infrastructure: power, transport, financial sector etc. is feasible.
- However, Cyber Capabilities **do not fit traditional security strategies** (deterrence, denial), because:
  - Problem of attribution of an attack
  - Rapidly evolving technology produced and in the hands of the private sector
- **Arms control agreements (so far) unrealistic** for cyber capabilities
  - Multiple actors, both state and non-state actors
  - No commonly accepted definition of a cyber weapon so far

“The Cyber Security Challenge: What Can be Done?”

- These scenarios show that we need:
  - to engage in an international discussion on **the norms and principles of responsible state behavior in cyber space**, including on the conduct of cyber warfare, and its possible exclusion or mitigation (Tallinn Manual a beginning)
  - In order to establish a universal understanding of the norms and principles of responsible state behavior in cyber space, we need to **turn to the United Nations** (such as UN GA, UNGGE, WSIS Geneva Action Line 5)
  - To **prevent an escalation** we need to develop **Confidence Building Measures CBMs** (e.g. Bilateral Agreements, OSCE, ARF, UN GGE)
  - Continue **the London – Budapest - Seoul Conferences** Process on Cyberspace to **create political awareness** and reach out to other regions and actors (through inter alia training)

Erosion of Trust

Trust between states and between state and citizens is increasingly **eroding** by a range of state practices, including with regard to the **negative uses of information communications technologies and related capabilities to advance political, military and economic goals.**

The interest in these state practises have inadvertedly also been **stoked** by developments such as:

-The role ICTs have played recently in **the Middle East and North Africa**;
- The alleged state use of sophisticated malware such **as Stuxnet** to achieve foreign policy goals;
- and Edward Snowden's disclosures on **the monitoring and surveillance practices**.

Despite a range of domestic and diplomatic efforts **initiated to curb such practices**, **many states have rushed to develop these same capabilities** to use not only against other states but against their own citizens, which further undermined confidence and trust between states, and between states and citizens.

WHAT COULD BE DONE ? CBMS AND CIVIL SOCIETY: WHY?

Over the past decades, there has been an increasing acceptance by governments of the principles of **transparency, participation and accountability in international policy making**.

However, to date, business and civil society **participation** (whether direct or indirect) in the development of national cybersecurity strategies or in regional and international CBM processes has **been minimal**, despite the fact that citizens, civil society organisations, as well as business and academia are a core link in the ICT value chain. Also, Civil society and academic expertise/ knowledge is fundamental to resolving many of the core technical problems inherent in the ICT.

Even international Conferences on Cyberspace such as the series launched in London in 2011 and continued in Budapest in 2012 and Seoul in 2013, aimed specifically at broadening the cybersecurity dialogue beyond government participants, has stalled, with a broad number of **civil society organisations left knocking at the door**.

At the same time, it is important to acknowledge also, that to a large extent, **civil society organisations came into the game rather late,** only making links between the international security dimensions of ICTs, and human rights, development and governance issues in recent years.

Where are we at today?

In 2013, the role of Civil Society and Industry was officially recognised in **the UN GGE Report** in the area of building cooperation for a peaceful, secure, resilient, and open ICT environment. More specifically: **Art. 11** acknowledges that 'while States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society'.

Moreover, the report's section on CBMs and Exchange of Information also acknowledges a role for civil society, specifically noting **in Art. 27** that 'while States must lead in the development of confidence building measures, their work would benefit from the appropriate involvement of the private sector and civil society'.

But then, when we look at **the OSCE's Decision 1106 on an 'Initial Set of CBMs to Reduce the Risks of Conflict Stemming from the Use of ICTs**' adopted il in December last year, no mention of civil society is made throughout the document. **However**, this does not necessarily mean that civil society should not play a role in implementing the initial set of CBMs. Indeed, the OSCE's own Guide on CBMs stresses how CBMs should ideally involve both government structures and civil society, with the latter also reaching out to broader society.

WHAT ROLE FOR CIVIL SOCIETY AND INDUSTRY IN FURTHERING CYBERSECURITY-RELATED CBMS, PARTICULARLY GIVEN THE UN GGE AND OSCE BREAKTHROUGHS?

Proposed areas of work for business and civil society**: i) Transparency and Accountability; ii) Participation; and iii) Deepening the Knowledge Base.**

i) **Transparency and Accountability**

Until very recently**, very little information regarding international, regional and bi-lateral processes on cybersecurity was in the public domain**. To a large degree, many of these discussions have received limited scrutiny from traditional sources of checks and balances, including business and civil society**. In this regard, business and civil society organisations can:**

-Develop tools to monitor their own government's role in international, regional and bi-lateral CBM and norm discussions.

-Make knowledge regarding progress or setbacks in international and regional CBM and norms processes readily available to the public and organise public discussions around them.

-Monitor budgetary expenditure in the field of cybersecurity to ensure an adequate balance of investment between security, governance, development and human rights).

For example, in May this year, **ICT4 Peace published its first annual Baseline Review of ICT-related events and processes** that have implications for international peace and security. A range of actors ranging from government officials to academia, advocacy organisations and business have welcomed the review as the first report of its kind covering the range of inter-connected policy areas – international and regional security; crime and terrorism; and governance, development and human rights.

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

Role for Civil Society and Industry (continued)

ii) Participation

While legitimate national security concerns have been raised concerning the non-public aspect of CBMs, norms and other related processes, there **are sufficient examples** of how governments and international and regional organisations have taken steps to make them more inclusive.

Business and Civil Society organisations can and should therefore:

- Lobby for their direct of indirect participation in CBMs, norms and other cybersecurity-related processes as per the related provisions in the 2013 GGE report. For instance**, civil society representation can and should be included in government delegations** to CBM and norm discussions.

- Where the latter is not possible, hearings with governments and civil society organisations should be organised, before and after government participation in CBMs, norms and other cyber-security-related processes. This is done in other areas pertaining to international peace and security, and there is no reason it cannot be done with regard to cybersecurity.

- Civil Society can also further CBMs by participating in capacity building efforts. For example, as a follow-up to the UN GGE Report and the Seoul Conference**, ICT4Peace is launching a new capacity building project with different regional organisations**. The objective of these capacity building efforts is to help level the playing field, ensuring that all regions are substantively and technically equipped to participate in international and regional ICT-related CBM and norms processes.

Role for Civil Society and Industry (continued)

iii) Deepening the Knowledge Base

Enhancing knowledge and sharing information is core to building a secure and resilient ICT environment, and for strengthening trust and confidence.

To this end civil society can:

Work more closely with the private sector and academia to ensure **that evidence-based research is made available to government representatives in CBMs** and norm discussions on the one hand; and made accessible to the broader public on the other.

For example, in June 2013, **ICT4Peace organised a workshop ETH Zurich on CBMs** and options for international and regional cybersecurity.
The workshop's combination of civil society, government, academia and business from different regions brought valuable perspectives from their own institutional experience within their own regional realities. The workshop participants drew up an exhaustive list of potential **CBMs across core areas: transparency measures; cooperative measures; communication and collaborative mechanisms; restraint measures; and compliance and monitoring measures for dealing with today's ICT-related challenges**. All of this information and analysis was pulled together in the ICT4Peace report on the workshop proceedings, copies of which I have with me here today, in case you are interested.

ICT4Peace Report on Transparency and Confidence Building Measures (TCBMs)**

** see Report by Camino Kavanagh, Senior Advisor ICT4Peace:
http://ict4peace.org/what-next-building-confidence-measures-for-the-cyberspace/
ICT4Peace workshop at ETH Zurich June 2013 with the Support of the Swiss Ministry of Foreign Affairs

Role for Civil Society and Industry (continued)

iii) Deepening the knowledge base

Civil Society and industry should develop stronger ties with academia and policy think tanks to identify knowledge gaps or deepen the knowledge base. For example, a number **of policy think tanks and civil society** organisations - including ICT4 Peace - are **supporting Track 1.5 or Track 2 consultations** in this field (i.e. consultation between Governments on Cybersecurity issues with the inclusion of academia, think tanks).

Civil Society should work with government, academia and industry to ensure **the inter-linkages between different policy areas, namely security, governance, development and human rights are understood and taken into account in negotiations.** As noted above, the ICT4 Peace Review of ICT-Related Processes and Events has played an important role in this regard.

Finally, civil society can **help deepening understanding of regional and cultural dynamics and differences as a means to build trust in cyberspace** and with regard to different cybersecurity challenges. Indeed, **significant misunderstandings (many of them cultural) still remain in the area of cybersecurity, which can lead to heightening of tensions between states, and between states and citizens if left unresolved.**

THANK YOU

danielstauffacher@ict4peace.org