OSCE

Meeting of the Informal Working Group Established by PC Decision 1039

Tuesday, July 21 2015, Hofburg, Ratsaal

Presentation by ICT4Peace Foundation on Cyber Training for Diplomats

Dr. Daniel Stauffacher President, ICT4Peace Foundation
ICT4Peace is a policy and action-oriented international Foundation. Our purpose is to save lives and protect human dignity through Information and Communication Technology.

We promote cybersecurity and a peaceful cyberspace through international negotiations with governments, companies and non-state actors. We also explore and champion the use of ICTs and media for crisis management, humanitarian aid and peace building.

To learn more about our activities and projects: [www.ict4peace.org](http://www.ict4peace.org)
The Role of ICTs in Preventing, Responding to and Recovering from Conflict

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

“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.
ICTs For Peaceful Purposes

Since WSIS 2005 in Tunis, a vibrant community of state and non-state actors has emerged. This community has developed a broad range of new ICT tools for peaceful purposes and in support of humanitarian operations.

These include tools such as crowdsourcing like Ushahidi, crisis mapping, two-way communications with victims of disasters and so forth.

In particular informal communities of expertise have contributed significantly to developing and deploying ICTs in support of crisis information management systems and peace-building efforts. But more work is needed.
ICTs Detrimental to Peace, Trust and Security

However, over the past decade we have also witnessed how ICTs are increasingly used for purposes detrimental to peace and security, including hacking and other attacks on digital networks and systems, use of ICT for terrorist purposes.

Traditional and social media are also being used to promote disharmony and conflict between and within countries and increasingly, to incite violence.

The step from common crime to politically motivated acts, even terrorism, is not far.
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.

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

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

- These scenarios show that Civil Society and Private Sector need, inter alia:

  - to engage in an international discussion on the norms and principles of responsible state behavior in cyber space,

  - To engage in developing Confidence Building Measures CBMs (e.g. Bilateral Agreements, OSCE, ARF, UN GGE)

  - to engage in the development of cooperation practises between Governments, Private Sector, Civil society to address cybersecurity challenges and develop cooperation models

  - Reach out and include all Regions of the world and in particular Developing Countries and include them in the reflection of, consultations and negotiations on norms, CBMs through CapaciltyBuilding
WHAT ROLE FOR CIVIL SOCIETY AND INDUSTRY IN FURTHERING CYBERSECURITY-RELATED NORMS AND CBMS, PARTICULARLY GIVEN THE UN GGE AND OSCE BREAKTHROUGHS?

Proposed areas of engagement for think tanks, academia, business and civil society inter alia:

• Deepening the Knowledge Base.

• Capacity Building for International Cyber Security Negotiations
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, academia and private sector can cooperate more:

- 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 participants from all over the world 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.
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
Deepening the Knowledge Base (continued)

For example, in 2014, ICT4 Peace published its first annual Baseline Review of ICT-related events and processes that have implications for international peace and security.

An up-dated version is being prepared for publication in fall 2015, based on a workshop at ETH Zürich in January 2015 with experts from inter alia Germany, Kenya, US, Russia, China, Switzerland, Ireland, Estonia, Netherlands, UK.
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
与信息通信技术相关进程及大事的基本回顾
——对国际和地区安全的影响
（2011-2013）

作者: 卡米诺·卡瓦纳（Camino Kavanagh）
蒂姆·毛瑞尔（Tim Maurer）
艾妮肯·提克-瑞格斯（Eneken Tikk-Ringas）

信息通信技术和平基金会
2014年·日内瓦
A ROLE FOR CIVIL SOCIETY?

ICTs, NORMS AND CONFIDENCE BUILDING MEASURES
IN THE CONTEXT OF INTERNATIONAL SECURITY

Camino Kavanagh and Daniel Stauffacher

GENEVA 2014
ICT4Peace Foundation
¿UN PAPEL PARA LA SOCIEDAD CIVIL?

TIC, NORMAS Y MEDIDAS DE CONSTRUCCIÓN DE CONFIANZA EN EL CONTEXTO DE LA SEGURIDAD INTERNACIONAL

Camino Kavanagh y Daniel Stauffacher

GINEBRA 2014
ICT4Peace Foundation
The Government of Kenya and ICT4Peace Foundation co-organize the first Regional Training Workshop in Africa on International Security and Diplomacy in Cyberspace

The ICT4Peace Foundation is honored to have been invited by the Government of Kenya to co-host the first regional training workshop in Africa (2 to 3 March 2015) on International Security and Diplomacy in Cyberspace with over 30 participants (Diplomats, Legal, Security and Technical Staff) from 12 African Countries, the African Union, and Civil Society Representatives. The workshop was co-chaired with Dr. Katherine Getao, Secretary, ICT Authority of Kenya. The Governments of Kenya, the UK, Germany and Switzerland supported the workshop course financially and with lecturers.

This new cyber security capacity building program was developed by the ICT4Peace Foundation as a direct follow-up to some of the recommendations tabled in the 2013 Report of the "UN Group of Governmental Experts on Cybersecurity in Cyberspace."
Capacity Building for International Cyber Security Negotiations


**ICT4Peace Cybersecurity policy and diplomacy course carried out so far in cooperation with:**

- OAS in Bogota for Latin America (November 2014),
- Government of Kenya for East African Countries in Nairobi (March 2015)
- Government of the Netherlands at the Hague Global Conference on Cyberspace (April 2015)

**Planned:**

- With Government of Singapore for ASEAN Countries (October 2015
- With African Union for African Countries (Ende 2015/Early 2016)
- With GCSP for Diplomatic Community in Geneva (March 2016)

With the generous support by the Governments of UK, Germany, Switzerland, Kenya, Netherlands, Singapore, Canada, US, Australia
Capacity Building for International Cyber Security Negotiations

Long Term Objective and Impact of the Workshop for Diplomats and Technical personnel:

Long Term Objective:
Mitigating risks to both rights and security in the cyber-sphere through the promotion of international norms of responsible state behavior, confidence-building measures (CBMs), and international cooperation.

The expected long-term impact:

1. More inclusive and knowledge-based debates, consultations or negotiations with and by all regions on norms and CBMs, with all stake-holders: Governments, industry, civil society, including academia;

2. More agreements at bilateral, regional at global level on norms, CBMs and international cooperation;

3. Progress towards a sustained open, prosperous, trustworthy, safe and secure cyberspace.
**Short Term Objectives:**

- A better and more detailed understanding by public officials, diplomats, industry, civil society representatives from all regions of the world of international norms, CBMs and international cooperation in the Cyber space;

- To broaden the participation in the international debates and regional and global negotiations in fora such as the London Process, UN GGE, OSCE, ASEAN, OAS, in the EU, the AU and AP-CERT;

- A better understanding of the concerns, best practices, policies and institutional arrangements in the field of cyber security at the regional level;

- Build a network of alumni, lecturers and experts of the workshop course, to up-date and exchange information on future developments in the global and regional international cyber security debate, research and negotiations.
Course Content:

• The Workshop Course provides an introduction to the subject of international cyber security negotiations and the current consultation and negotiation efforts.

• Participants will be exposed to the context in which cyber security is being addressed in global forums, such as the UN GGE, OSCE, OAS, ARF, AU and consider the key issues raised.

• A simulation element will provide an active learning opportunity in which participants will try to develop a consensus text on a specific principle central to the current inter-state debate on cyber security.

• The workshop course will provide an opportunity for the participants and the lecturers to discuss and learn of the concerns, best practices and policies at the regional level.
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00-09:30</td>
<td>Welcome, Workshop Overview and Objectives, Introductions</td>
</tr>
<tr>
<td>09:30-10:30</td>
<td>International Cyber Security: Background &amp; Context</td>
</tr>
<tr>
<td>10:30-11:00</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>11:00-12:30</td>
<td>Cyber Security &amp; International Law</td>
</tr>
<tr>
<td>12:30-14:00</td>
<td>Lunch</td>
</tr>
<tr>
<td>14:00-15:30</td>
<td>Building confidence between states, including the role of</td>
</tr>
<tr>
<td></td>
<td>International and Regional Organizations</td>
</tr>
<tr>
<td>15:30-16:00</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>16:00-17:45</td>
<td>Discussion of Regional Perspectives and Policy Options Q&amp;A</td>
</tr>
<tr>
<td>17:45-18:00</td>
<td>Introduction to the Exercise</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00-10:30</td>
<td>Exercise</td>
</tr>
</tbody>
</table>

Coffee served in meeting room

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30-11:30</td>
<td>Continuation and Review of Exercise</td>
</tr>
<tr>
<td>11:30-12:15</td>
<td>General Discussion on Lessons Learned and the Way Forward for Africa</td>
</tr>
<tr>
<td>12:15-12:30</td>
<td>Closing</td>
</tr>
</tbody>
</table>
Cybersecurity and the International Law:

The international dialogue on responsible State behavior e.g.:

• Background and process in the UN Ist Committee (UN GGE)
• The framework of applicability of international law: from whether it applies to how it applies (sovereignty, state responsibility, peaceful settlement of disputes, human rights)
• politically binding norms for responsible State behavior

The applicability of LOAC e.g.:

• prohibition of the use of force
• right to self-defence
• Principles of necessity, proportionality, distinction,
Confidence Building among States including the role of International and Regional organisations.

The CBMs discussion focused on e.g.:

- Background and concept of confidence-building;
- Examples 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.
- Examples of cyber CBMs based on the UN Ist Committee process, the OSCE set of CBMs and other regional initiatives.
THANK YOU
danielstauffacher@ict4peace.org