22nd International Association of Prosecutors Annual Conference

Beijing 12 September 2017

Dr. Daniel Stauffacher, President, ICT4Peace Foundation
www.ict4peace.org
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
The UN World Summit on the Information Society (WSIS) in Geneva 2003 Tunis 2005

• Paragraph 36 of the World Summit on the Information Society (WSIS) Tunis Commitment (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.”
Information and Communication Technology for Peace

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

Preface by
Kofi Annan

Foreword by
Micheline Calmy-Rey

By Daniel Stauffacher, William Drake,
Paul Currion and Julia Steinberger
ICT4Peace’s interlinked Areas of Work:

1. Since 2004 using ICTs, new media etc. by the international community/UN for Peaceful Purposes inter alia humanitarian operations, peace-keeping and peace building;

2. Since 2007 Promotion of Peace and Security in the Cyberspace (to maintain an open, secure, stable, accessible and peaceful ICT environment (International Law, Norms, CBMs, Capacity Building, Tech Against Terrorism).
UN Secretary-General 2010 Crisis Information Strategy (A/65/491)

• 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 Support (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.
The Cybersecurity Challenge

• Many states are pursuing military cyber-capabilities: UNIDIR Cyber Index: more than 114 national cyber security programs worldwide, more than 45 have cyber-security programs that give some role to the armed forces.

• A private can obtain, train and use cyber weapons of war.

• Damaging of a country’s certain critical infrastructure: power, transport, financial sector etc. is possible.

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

• An exclusive, all-out cyber-war has not happened yet, but attacks have happened as part of conflicts

• 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
  - Use of Non-State actors, Proxies

• 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.

  - 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).

  - We need Capacity Building at all levels (policy, diplomatic and technical) to include also developing and emerging countries.
Getting down to business
Realistic goals for the promotion of peace in cyber-space

A Code of conduct for Cyber-conflicts

Daniel Stauffacher, Chairman, ICT4Peace Foundation & Former Ambassador of Switzerland
Riccardo Sibilia, Head of Cyber Threat Analysis, Swiss Armed Forces, Switzerland
Barbara Weekes, CEO, Geneva Security Forum

ICT4Peace Foundation

December 2011

¿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

BASELINE REVIEW
ICT-RELATED PROCESSES & EVENTS
IMPLICATIONS FOR INTERNATIONAL AND REGIONAL SECURITY
(2011-2013)
Camino Kavanagh, Tim Rouwer and Enekem Titi-K'Ringas

CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY

Seventieth session
Item 93 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
UN Group of Governmental Experts (GGE) on Cybersecurity – 2015: First Set of Peace time norms of responsible State behaviour

• 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’.

• A State should not conduct or knowingly support ICT that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public

• States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

• States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats.

• At the same time, 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.'
DECISION No. 1202

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
Confidence Building Measures: Important Progress at OSCE (CH Presidency)

• Nominating contact points;

• Providing their national views on various aspects of national and transnational threats to and in the use of Information and Communication Technologies;

• Facilitating co-operation among the competent national bodies and exchanging information;

• Holding 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 Information and Communication Technologies;

• Sharing information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet, and on their national organization; strategies; policies and programs;

• Using the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building;
ICT4Peace Cybersecurity policy and diplomacy capacity building program with different regional organisations.

As part of its Capacity Building Program for International Cyber Security Negotiations, ICT4Peace organised in cooperation with the African Union Commission the first cybersecurity policy and diplomacy workshop at The African Union Headquarters in Addis Ababa on 15 and 16 February 2016 (see AU Press release).

43 mid-level and senior diplomats from 28 English and French speaking African Countries and 3 regional organisations participated in the 1 1/2 days workshop. The teaching faculty included high-level diplomats and experts from Kenya, Estonia, Switzerland, Germany, Australia and Finland. The workshop was made possible thanks to the generous financial support from the Government of the UK and the AU Commission. Switzerland, Germany, and Australia made high-level experts available.

The workshop program can be found here. and covered the following areas:

- Current international cyber security policy issues
- National cyber security strategies
- Current cyber security consultations and negotiation efforts at the global, regional and bilateral levels
- Cyber security and international law
- Norms of responsible State behaviour in cyber space
- Confidence Building Measures (CBMs) and the role of international and regional organisations
The Cyber Security Agency (CSA) of Singapore, in collaboration with ICT4Peace Foundation, held the inaugural ASEAN Cyber Norms Workshop in Singapore from 8 to 9 May 2017 under the auspices of Singapore’s ASEAN Cyber Capacity Programme.

This Workshop aimed at launching a regional conversation on the promotion of (1) norms of responsible behaviour by states and non-state actors in the cyberspace, and (2) the use of ICTs for peaceful purposes by providing an opportunity for participants from ASEAN countries to receive updates on and discuss significant recent developments in international cybersecurity norms discussions, including those at the UN Group of Governmental Experts (UN GGE) on Developments in the field of Information and Telecommunications in the context of International Security.

In addition to forty senior-level participants from ASEAN Governments, thirteen Senior Diplomats from and Experts from Australia, China, Egypt, Germany, Indonesia, Japan, Malaysia, Netherlands, United States, Finland and Estonia participated. These countries are also members of the ongoing UN GGE. ICT4Peace, which was invited by Singapore to collaborate in the organisation of this workshop, was represented by Dr. Eneken Tikk, Dr. Mika Kerttunen and Dr. Daniel Stauffacher.
Connecting industry, government, and civil society to prevent the terrorist use of the internet whilst respecting human rights

**techagainstterrorism.org**  **@techvsterrorism**

A joint project implemented by UN CTED and ICT4Peace Foundation under mandate of the United Nations Security Council Counter-Terrorism Committee
Security Council and Counter-Terrorism Committee Mandate

• Resolution 2129 (2013) Notes the evolving nexus between terrorism and information and communications technologies, in particular the Internet, and the use of such technologies to commit terrorist acts, and to facilitate such acts through their use to incite, recruit, fund, or plan terrorist acts, and directs CTED to continue to address this issue, in consultation with Member States, international, regional and subregional organizations, the private sector and civil society and to advise the CTC on further approaches.

• In April 2017, the CTC submitted to the Security Council a proposal for a comprehensive international framework to counter terrorist narratives (S/2017/375) pursuant to the Presidential Statement S/PRST/2016/6. The CTC proposal mentioned public-private partnership as an important element to counter incitement and described the TechAgainstTerrorism initiative as a good practice.
In 2016 we laid the foundations for the Tech Against Terrorism Project through a series of global workshops

1. Identify the terrorist threats
   - How are terrorists exploiting tech?
   - What are the most important areas to consider our work?

2. Understand tech responses
   - How are tech companies responding?
   - What are the strengths and weaknesses?
   - What can we learn?

3. Stakeholder responses
   - How can we support multi-stakeholder engagement?
   - How can we listen to human rights and civil society?

4. Supporting tech and startups
   - What can we do to provide operational support to tech and startups?
   - How can we inform States about the best approaches?
We held workshops in Zurich, Silicon Valley, and Kuala Lumpur
In this project we are focusing on tech organisations that can be exploited by terrorists to publicise, recruit, and support operations.

1. Publicity and recruitment
   - Social media and sharing platforms

2. Operational usage (overt / covert)
   - Communications and messaging
   - Content storage and knowledge sharing
   - Financial funding and transfers
ICT4Peace Global workshops included industry representatives from technology, media, telecommunications, and finance.
ICT4Peace Global workshops included governments and intergovernmental organisations and agencies
ICT4Peace Global workshops included leading civil society organisations and human rights groups
ICT4Peace Global workshops included academic institutions and think tanks who contributed papers for each of the meetings
We presented our summary report for Phase 1 at the UN CTC in December 2016

http://bit.ly/2kMBDZJ

Google: UN private sector engagement ICT For Peace
Through our consultations a number of concerns were raised including the limited resources and capacity of startups

- Respect for human rights
- Evidence-base of impact is limited
- Significance of OFFLINE
- Startups have limited capacity
Large tech companies have developed an “emerging normative framework” to help tackle the terrorist use of tech

1. Terms of Service & Respect for Rights
   - Community guidelines and standards respecting freedom of expression and human rights principles
   - Operational definitions of violent extremism and terrorism

2. Content Takedowns
   - Content reporting by users, NGOs, and governments
   - Engagement with law enforcement
   - Engagement with Internet Referral Units (IRUs)
   - Careful deliberation of what content / accounts to take down given ToS

3. Transparency Reports
   - Regular reports of government and user-generated take-down requests
   - Transparency around government requests as protection against censorship concerns
Startups, however, often lack the capacity to set up effective defences and respond quickly to terrorist exploitation.

We aim to provide support...

1. Inform the debate and understand requirements
   - Promote the project
   - Engage startups
   - Organise workshops
   - Create guide / startup primer
   - Risks / Challenges

2. Provide operational advice and know-how in the short term
   - Case studies and networking
   - Data Science Network
   - Operational advice
   - ToS advice

3. Build online tools to help in the long term
   - Assessment tools
   - ToS Creator & Pledge
   - Trustmark
   - Standardised reporting formats
We developing an online Knowledge Sharing Platform (KPS) and facilitating ongoing engagement with the wider tech industry

2 Knowledge Sharing Platform  
Multi-Stakeholder Facilitation

Ongoing multi-stakeholder engagement

• Work with the GIFCT and stakeholders from civil society, academia, tech, government, law enforcement to facilitate dialogue and meaningful capacity building

Tech sector outreach and engagement

• Develop a network within the global tech industry to learn needs and to support through advice and ongoing knowledge sharing

Develop best practices and build practical tools

• Terms of Service, The Pledge  
• Guidelines & Primers for Startups  
• Advice on Operational Processes e.g. translation, moderation  
• Practical tools / tech, threat alerts, transparency reports

Support counter-speech

• Learn from counter-speech initiatives and further empower the tech industry and civil society to engage in this work
• Tech Against Terrorism is supporting the GIFCT to facilitate knowledge-sharing and multi-stakeholder engagement

Global Internet Forum to Counter Terrorism

1. Industry-led Technology
   - Enforcement optimisation
   - Hash sharing
   - Reporting / transparency

2. Knowledge Sharing, Facilitation
   - Multi-stakeholder engagement
   - Tech sector outreach, engagement, networking
   - Best Practices and Tools
     • Terms of Service, Pledge
     • Guidelines & Primers
     • Operational Processes
     • Practical tools, technologies, threat alerts, transparency
   - Counter-speech

3. Research
   - Engagement with and commission of research by global CT experts

Senior leadership-led forum engagement
Merci Beaucoup

danielstauffacher@ict4peace.org