ICT4Peace Foundation

University of St. Gallen, Switzerland, 3 December 2015

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

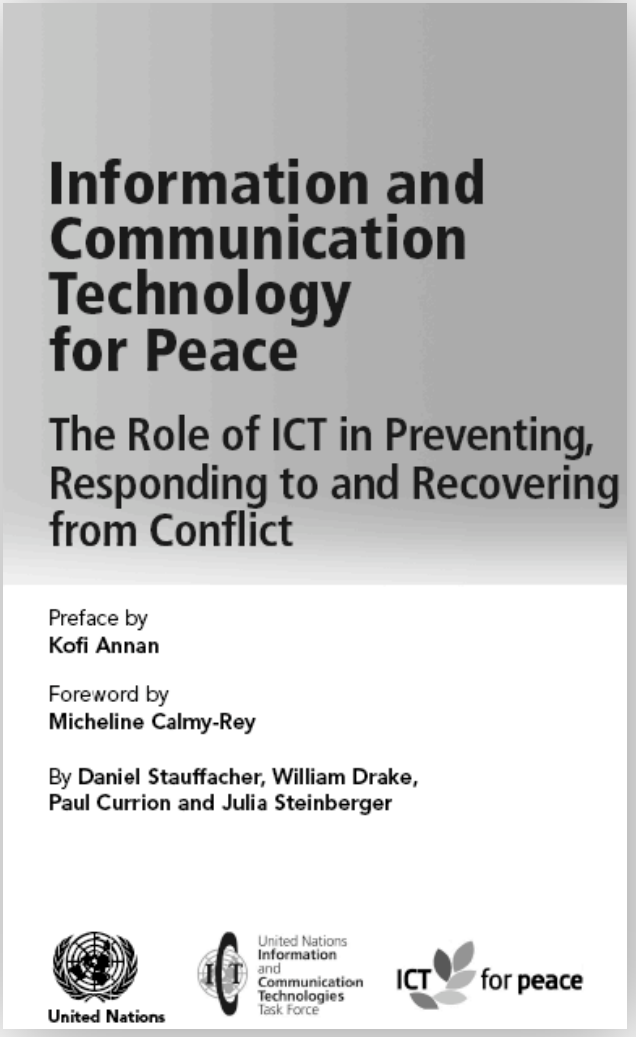
ICT for peace foundation

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.

ICT for peace 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**

ADVOCACY CAPACITY BUILDING STAKEHOLDER MANAGEMENT TECHNOLOGY DEVELOPMENT

THE ICT4PEACE FOUNDATION TEAM

The Foundation's advisory board consists of a Nobel Peace Laureate, senior diplomats, world-renowned practitioners, industry and domain experts, academics and researchers in the use of ICTs for peacebuilding and humanitarian aid.

Daniel Stauffacher

President

Martti Ahtisaari

Chairman, International Advisory Board

Barbara Weekes

Board Member

Maria Cattaui

Chairperson, ICT4Peace Foundation

Alain Modoux

Vice-Chairperson, ICT4Peace Foundation

Sanjana Hattotuwa

Special Advisor

Nigel Snoad

Board Member

Nitin Desai

Board Member

Shahid Akhtar

Board Member

Dag Nielsen

Board Member

Linton Wells II

Board Member

Michael Møller

Member of the Board, ICT4Peace Foundation

Satish Nambiar

Board Member

Kristiina Rintakoski

Board Member

Juliana Rotich

Board Member

Kamal Sedra

Senior Technical Advisor

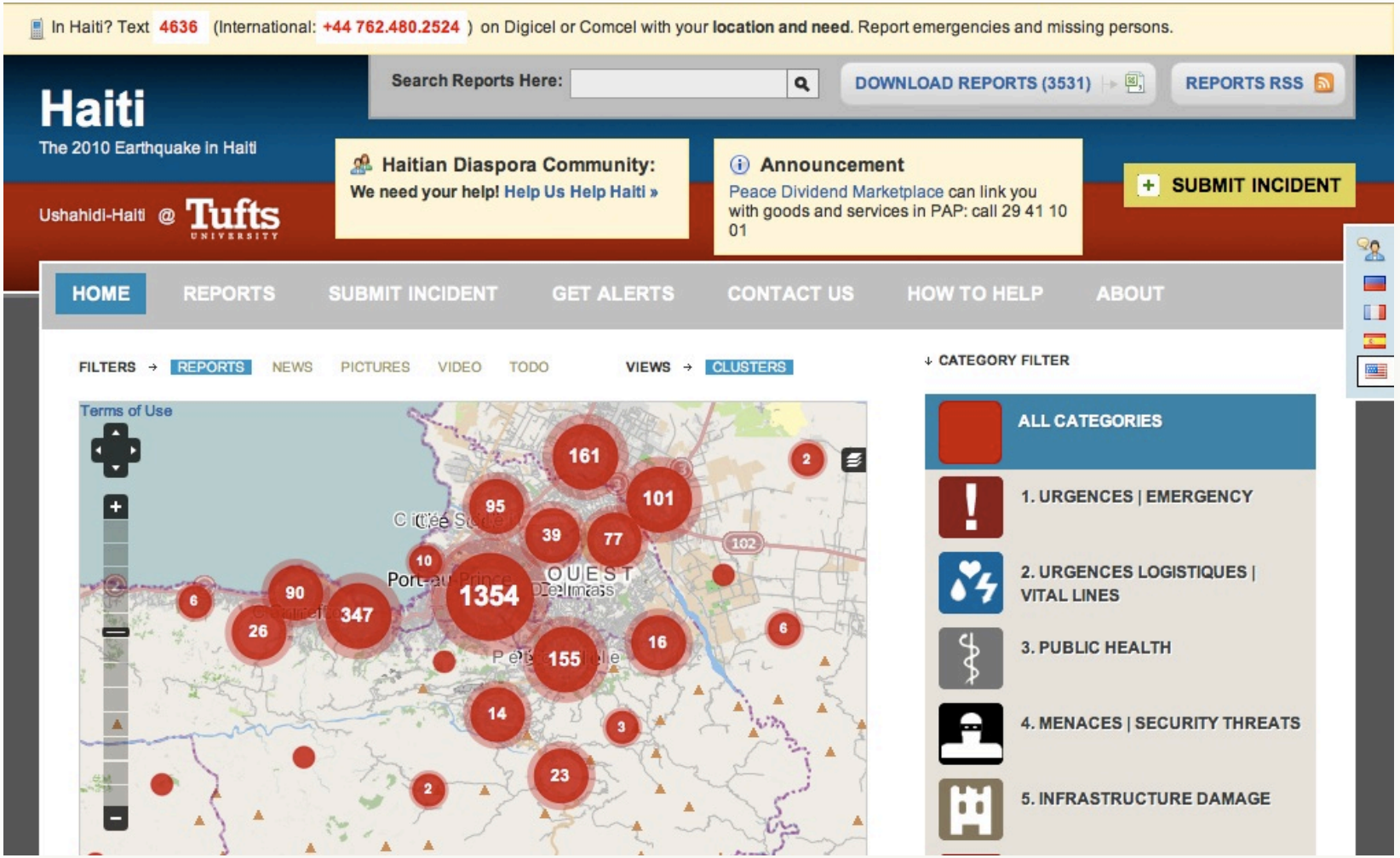
ICT4Peace interlinked Areas of Work:

1. CRISIS Information Management including using ICTs, new media etc.

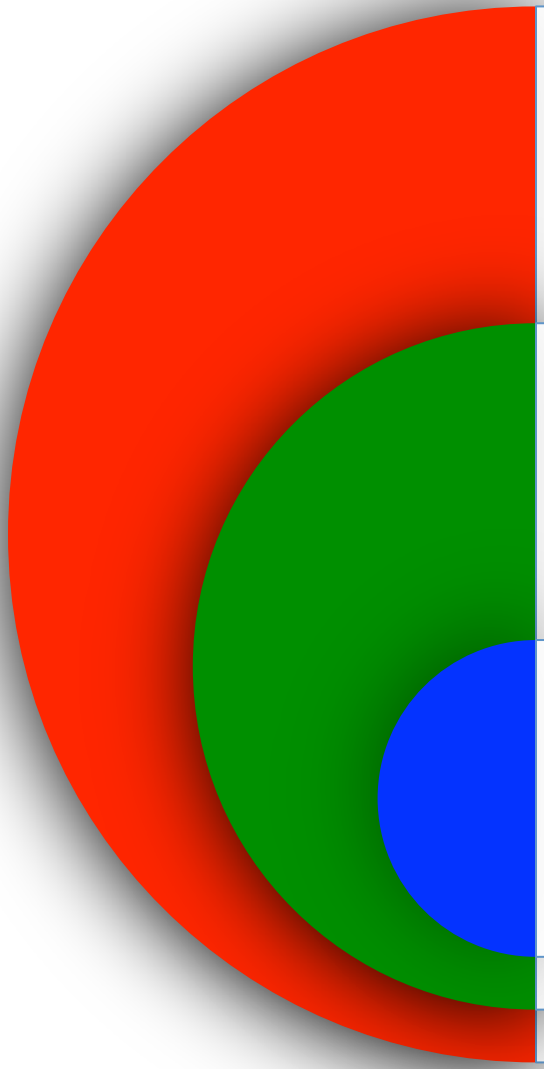
2. Cyber Security

ICT for peace foundation

New Tools: Mapping and Crowdsourcing for CiM - Learning from Kenya 2007, Haiti 2010, Libya, Typhoon Yolanda etc. etc.



Information break-down in crisis situation



New media

- Twitter
- Flickr
- Blogs
- SMS / MMS / Mobiles
- Social networks
- GIS

Mainstream media

- CNN / BBC / Al Jazeera
- Local / National TV and radio
- Print media (mainstream / regional)
- Alternative print media

Traditional Sources

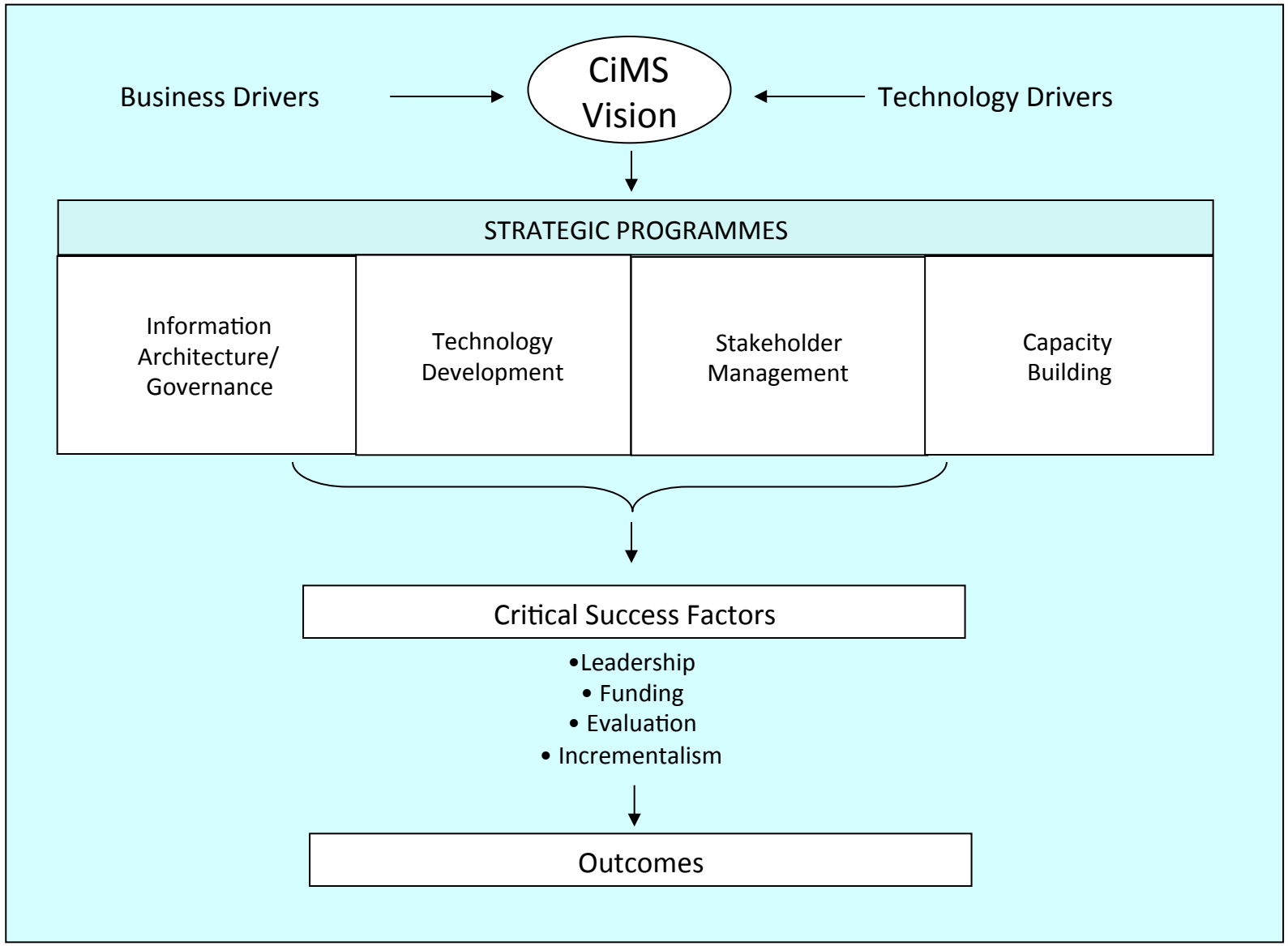
- Sit reps
- Open Data Open Gov Data
- Humanitarian Information Centres
- Agency databases / email lists
- Personal contacts / relationships

UN Crisis Information Management Advisory Group (CIMAG)

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 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.***


Business Drivers
CiMS Vision
Technology Drivers
STRATEGIC PROGRAMMES
Information Architecture/ Governance
Technology Development
Stakeholder Management
Capacity Building
Critical Success Factors
•Leadership
• Funding
• Evaluation
• Incrementalism
Outcomes

Improving Crisis Information Management in the Field: MONUSCO DRC CONGO

Situational awareness is critical to effective operations and informed decision-making as well as the safety and security of our personnel. Hosted by MONUSCO, in cooperation with the Department of Field Support, and facilitated by the ICT4Peace Foundation, the Improving Situational Awareness Workshop & Training will offer a collaborative forum to discuss information sharing principles, strategies and technologies with MONUSCO practitioners and UN partners.

This three day intensive workshop will introduce participants to new technology tools and platforms used in the collection, verification, and dissemination of information to improve situational awareness. Opportunities for information sharing within the mission and between UN partners will be identified and discussed to develop a practical roadmap for improvement.

CiM Training Course for IM using ICTs and big data, social and new media, ENTRI Course in Cooperation with ZIF and FBA

Navigate a new paradigm: Crisis Information Management Training Course

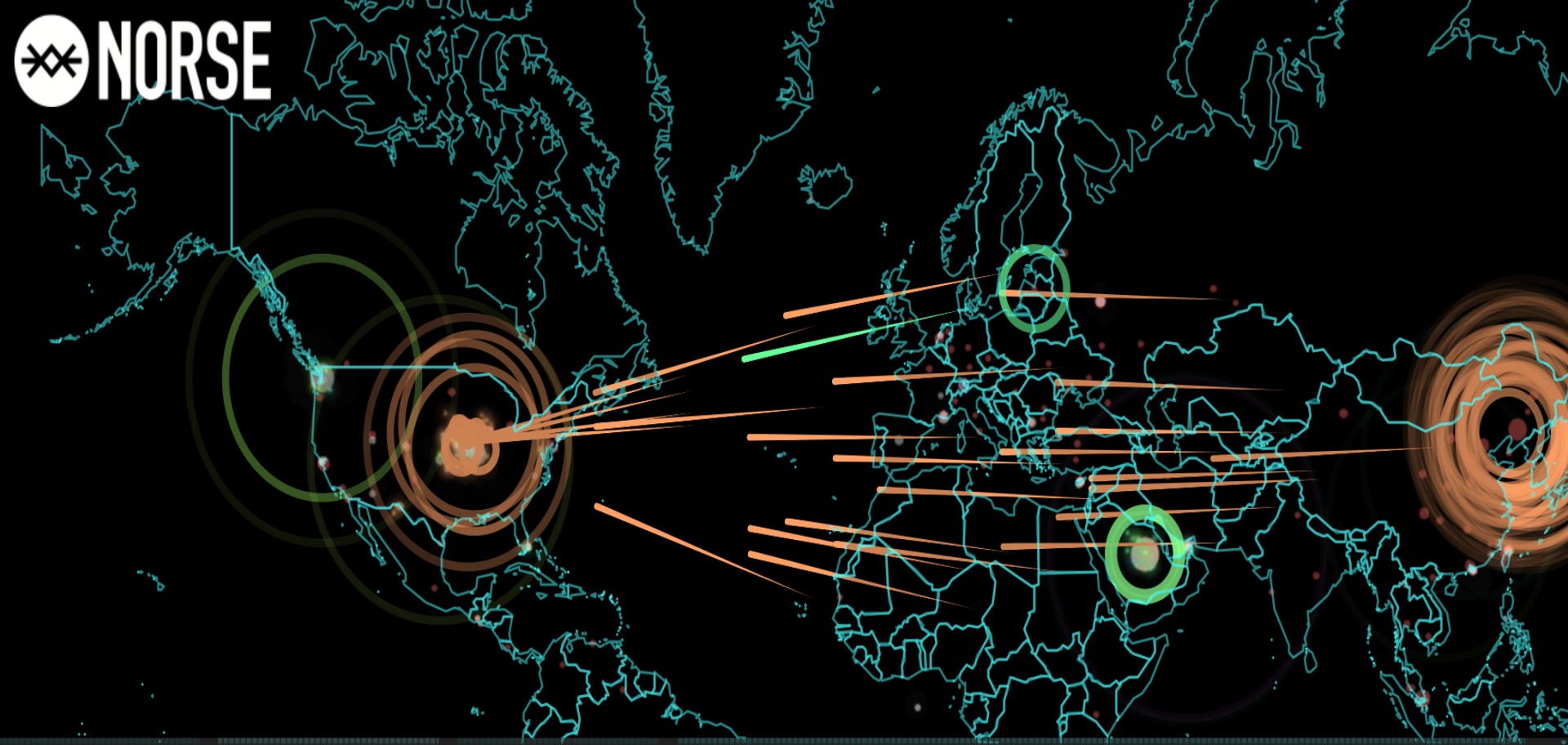
Folke Bernadotte Academy (FBA), Zentrum für Internationale Friedenseinsätze (ZIF) and ICT4Peace Foundation announce the new Crisis Information Management Training Course at the International Peace Support Training Center (IPSTC), Nairobi from 23 February to 3 March 2013. The Course will teach Information Management practices in Crisis, including Peace and Humanitarian Operations.

A special focus will be given to the use of new Media, including SMS, Twitter, crowd sourcing and crisis mapping to obtain manage and share data. This Course is also linked to the UN Crisis Information Management Strategy Implementation.

For more information, click on the image below.

Course Description

Efficient and timely provision of Shared Situational Awareness (SSA) and Crisis Information Management (CIM) are essential to enable effective decision-making in Multi-



ATTACK ORIGINS

#	COUNTRY
354	Saudi Arabia
336	China
168	United States
71	Singapore
44	Russia
43	Brazil
30	Taiwan
17	Netherlands
8	Germany
7	France

ATTACK TYPES

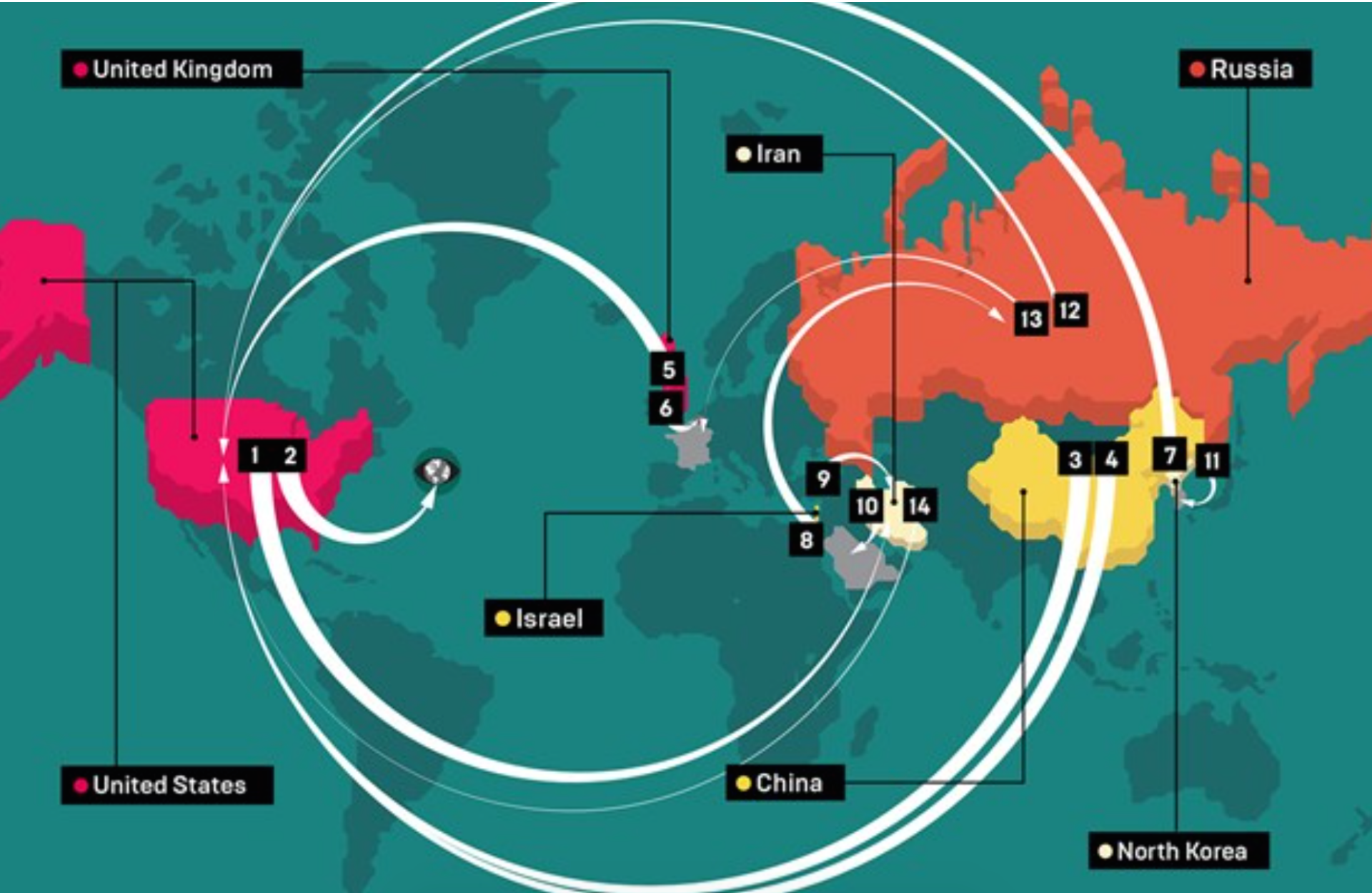
#	PORT	SERVICE TYPE
311	137	unknown
172	23	telnet
88	50864	unknown
69	445	microsoft-ds
55	50856	unknown
38	1500	vlsi-lm
35	33434	unknown
33	27017	unknown
24	443	ssl
21	17	qotd

ATTACK TARGETS

#	COUNTRY
648	United States
354	Saudi Arabia
30	Liechtenstein
30	France
26	United Arab Emi...
20	Russia
15	Taiwan
15	Bulgaria
11	Hong Kong
11	

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
09:00:24.256	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.262	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.267	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.322	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.328	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.332	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.507	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.513	Rn Data Sia	195.3.144.102	Riga, LV	San Francisc...	vnc	5900
09:00:24.518	National Computer Systems Co.	46.151.208.26	Riyadh, SA	Riyadh, SA	vlsi-lm	1500
		.66	Riyadh, SA	Riyadh, SA	unknown	137


United Kingdom
Russia
Iran
1
2
5
6
12
13
3
4
7
11
9
10
14
8
Israel
United States
China
North Korea

Cybersecurity Incidents

(Wired Magazine: http://www.wired.co.uk/magazine/archive/2015/10/start/infoporn-cyberattacks-state-sponsored-hacking)

1. UNITED STATES **2001-2015:** Target: the world. Seriously, the **NSA's reach appears to be limitless, according to documents leaked by Edward Snowden**, which describe a vast hacking operation aimed at subverting the internet's infrastructure.

2. UNITED STATES **2007: The US launched the Stuxnet worm against Iran to sabotage that country's nuclear program**.
Outcome: Stuxnet succeeded in briefly setting back the Iranian nuclear programme. The attack set a precedent for cyberwarfare: countries now launch digital assaults to resolve political disputes.

Cybersecurity Incidents

(according to Wired Magazine)

3. CHINA**2009-2011: China allegedly hacked Google, RSA Security and others to get the source code**. The hackers who breached RSA obtained core data used in the company's two-factor authentication scheme used by governments and corporations.

4. CHINA **2014: China breached several databases belonging to the US Office of Personnel Management**. The hackers stole sensitive data, including Social Security numbers, relating to more than 21 million people who had been interviewed for government background checks.

5. UNITED KINGDOM **2009-2013: The UK hacked Google's and Yahoo's undersea cables to siphon unencrypted traffic**. According to documents leaked by Edward Snowden, the UK accessed data through taps of undersea cables belonging not just to these companies, but to major telecoms too.

Cybersecurity Incidents

(according to Wired Magazine)

6. UNITED KINGDOM **2012:** The **UK's Government Communications Headquarters (GHHQ) hacked Belgacom to monitor all mobile traffic passing through its routers.**

7. NORTH KOREA **2014:** **Sony Pictures Entertainment was attacked.** The US attributed it to North Korea and applied additional sanctions against the country and specific officials.

8. ISRAEL **2014: Israel allegedly hacked Russian security firm Kaspersky Lab to obtain intel on its research about nation-state attacks.** It also struck venues in Europe where the UN Security Council met to negotiate Iran's nuclear programm.

Cybersecurity Incidents

(according to Wired Magazine)

9. ISRAEL **2012: Suspected of launching the Wiper attack against the Iranian oil ministry and the National Iranian Oil Company.**

10. IRAN **2012: Iran allegedly launched a virus called Shamoon against oil conglomerate Saudi Aramco's computers**. US officials blame Iran for the attack but have not produced evidence.

11. NORTH KOREA **2013: Computers in South Korea were struck by a logic bomb that caused data deletion as well as preventing rebooting. South Korea blamed North Korea for the attack but it has never produced solid evidence.**

Cybersecurity Incidents

(according to Wired Magazine)

12 RUSSIA **2014: Russia allegedly hacked the US State Department and the White House. The attackers had access to unclassified emails for President Obama as well as non-public details about his schedule.**

13. RUSSIA **2015: TV5Monde, a French-language broadcaster, is hacked -- reportedly by Russia. A group calling itself the CyberCaliphate took credit, but French officials have pointed the finger at the Kremlin**. The hackers blacked out broadcasting for several hours and posted messages expressing support for ISIS to the TV channel's social-media accounts.

14. IRAN **2011-2012: Iran launched a series of denial--of-service attacks on US banks. Although Izz ad--Din al-Qassam Cyber Fighters took responsibility, US officials claimed Iran was retaliating for Stuxnet and UN sanctions.**

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.

The Cybersecurity Challenge

- Numerous states are pursuing military cyber-capabilities: UNIDIR Cyber Index**: more than 114** national cyber security programs world-wide, more than **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.

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 **Central Europe Eastern Europe 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.

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**

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

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'.

- The Group noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an International Code of Conduct for Information Security, circulated by the Secretary-General as UN document A/69/723.

- 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.

A Comprehensive Normative Approach to Cyber Security

Presented at GCCS 2015

International norms

Legal (binding) norms		Political (non-binding) norms	
Hard law	Soft law		Non-legal norms
Binding norms (treaties, custom, general principles)	Binding norms with a soft dimension*	Non-binding norms of legal relevance*	Non-binding or voluntary norms (e.g. CBMs)

* See Fabien Terpan, *Soft Law in the European Union—The Changing Nature of EU Law,* European Law Journal, Volume 21, Issue 1, pages 68–96, January 2015

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

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;

BILATERAL EFFORTS IN THE FIELD OF INTERNATIONAL AND REGIONAL SECURITY
Track 1, 1.5 and 2 Dialogues

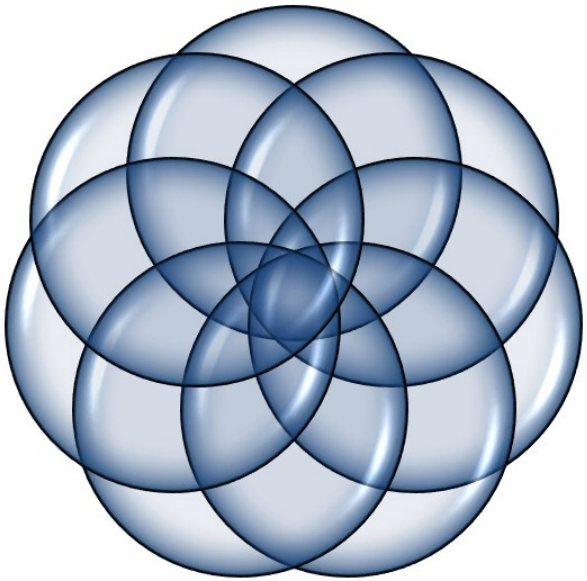
UNITED STATES
- Brazil
- China
- India
- Japan
- Russia
- Sth. Korea

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

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/)

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 work for think tanks, academia, business and civil society**:**

i) Transparency and Accountability;
ii) ii) Participation;
iii) and iii) Deepening the Knowledge Base.

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

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

ICT for peace
FOUNDATION

网络政策
进展概要

与信息通信技术相关进程&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

ICT for peace

CYBER SECURITY POLICY PROCESS BRIEF

¿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

ICT for peace

CYBER SECURITY POLICY PROCESS BRIEF

¿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

ICT4Peace Cybersecurity policy and diplomacy capacity building program with different regional organisations.

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

Vielen Dank

danielstauffacher@ict4peace.org