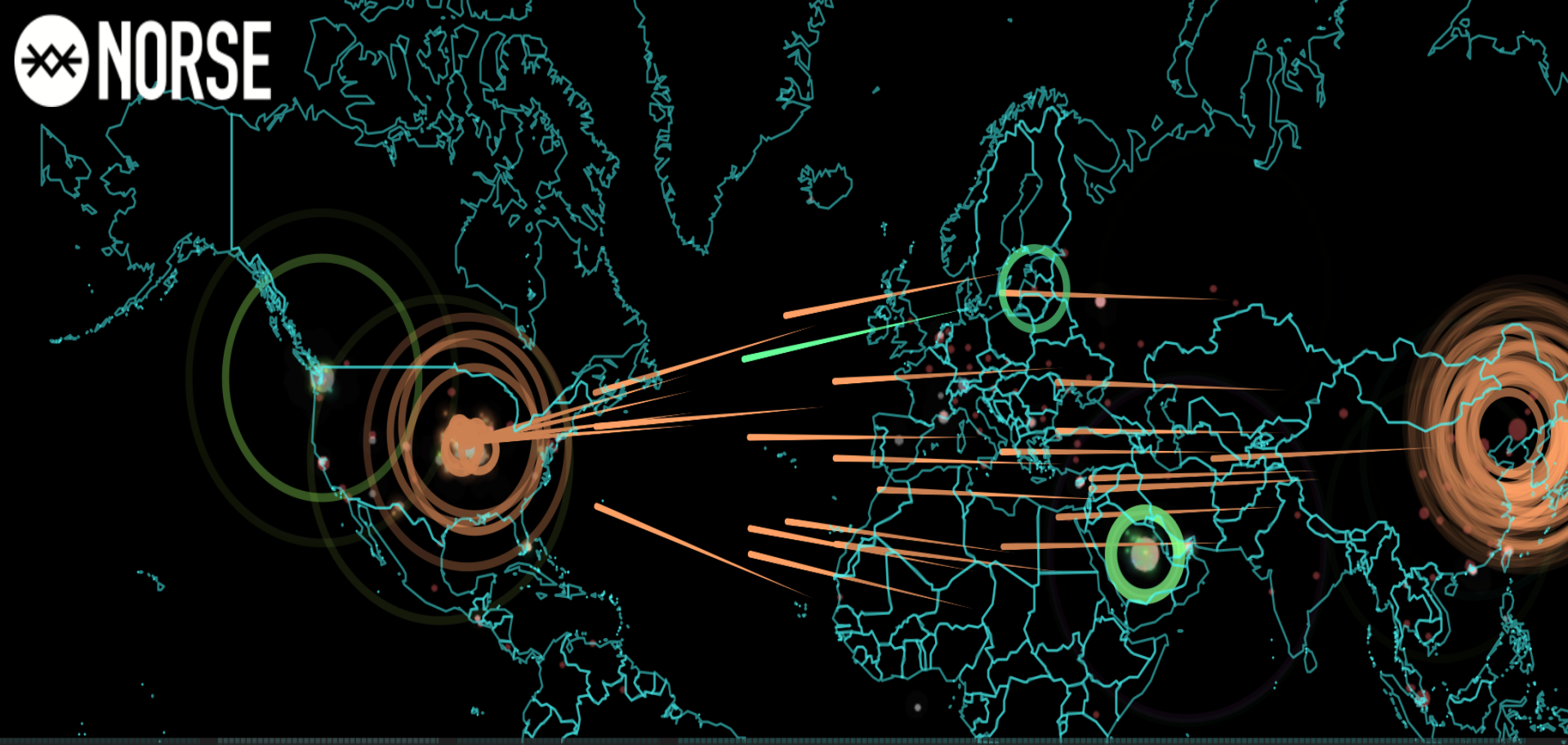
“The Cyber Security Challenge: What Can be Done?”

Swiss Business Association Singapore
Grand Hyatt, 22 October 2015

Presentation by Daniel Stauffacher
President, ICT4Peace Foundation
www.ict4peace.org

ICT for peace foundation



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

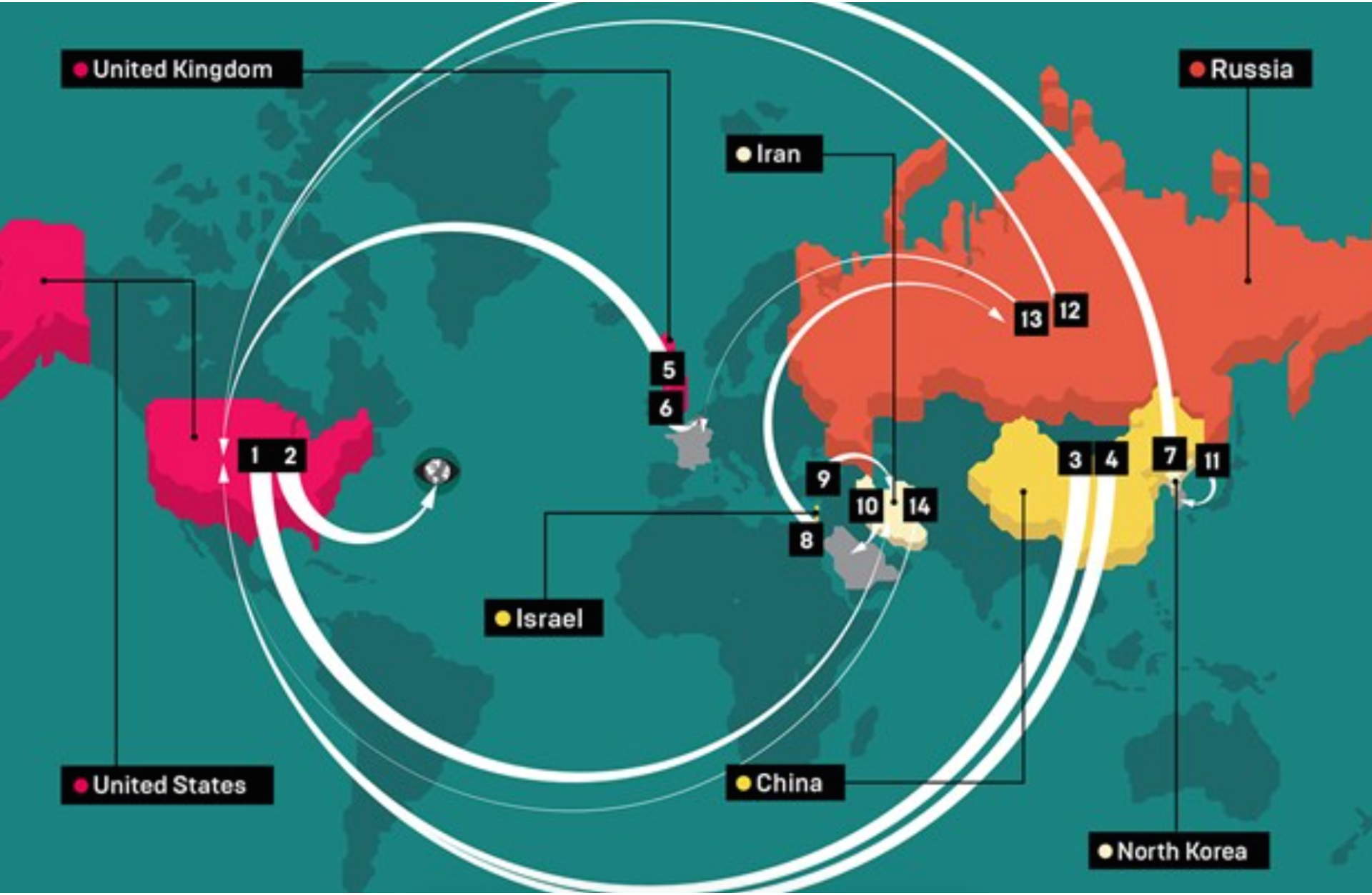
#	PORT	SERVICE TYPE
311	137	unknown
172	23	telnet
88	50864	unknown
69	445	microsoft-ds
55	50856	unknown
38	1500	vlsi-lm
35	33434	unknown
33	27017	unknown
24	443	ssl
21	17	qotd

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

(Based on article by 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.

The Cybersecurity Challenge

- **Many states are pursuing military cyber-capabilities**: **UNIDIR Cyber Index: more than 114** national cyber security programs world-wide, 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: 2007 against Estonia, 2008 against Georgia, 2010 against Iran, 2013 against South Korea, 2014 in Ukraine. In the context of the Syrian war, denial-of-service attacks have been reported.

- 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 (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)
  - **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 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.

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

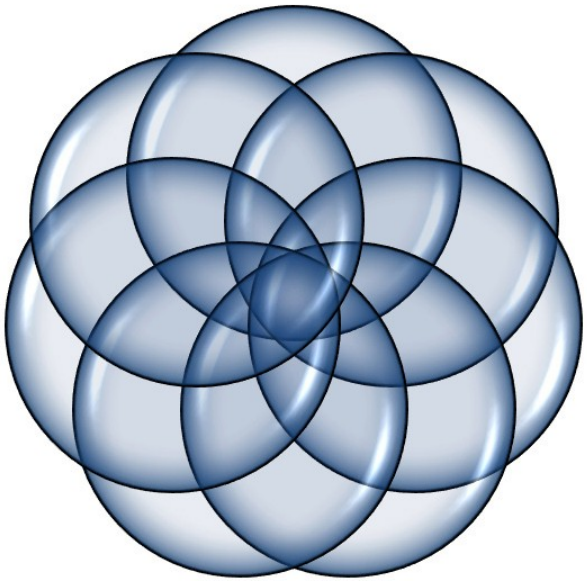
UNITED STATES
- Brazil
- China
- India
- Japan
- Russia
- Sth. Korea

UNITED KINGDOM
- China
- India

SOUTH KOREA
- US
- India

RUSSIA
- US
- India
- Brazil

BRAZIL
- Russia
- US

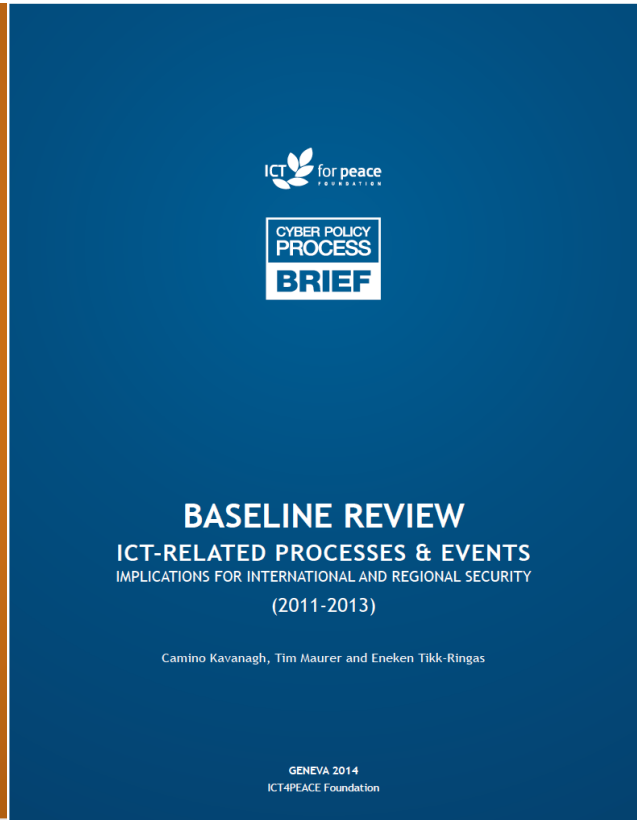


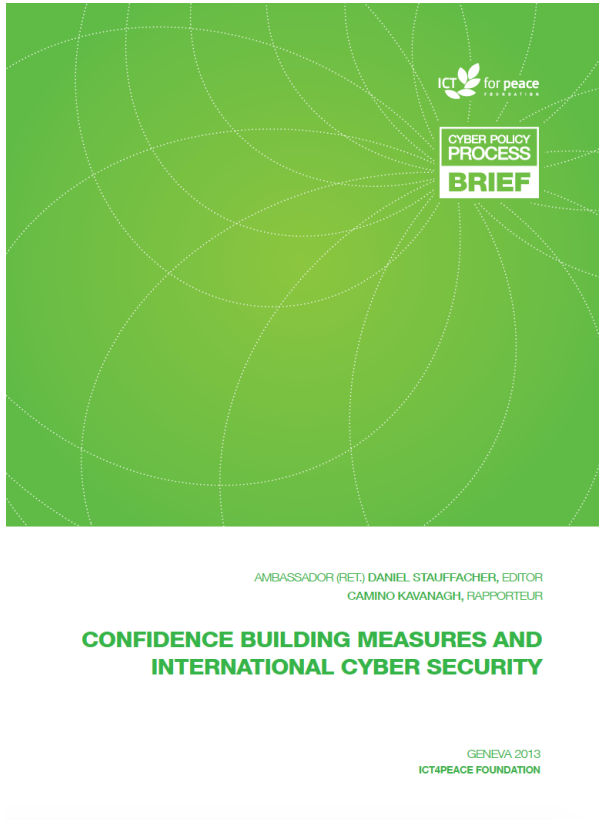
CHINA
- UK
- US
- EU
- Germany

GERMANY
- US
- India
- China

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

ICT4Peace Policy Research on Peace, Trust and Security in Cyberspace





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

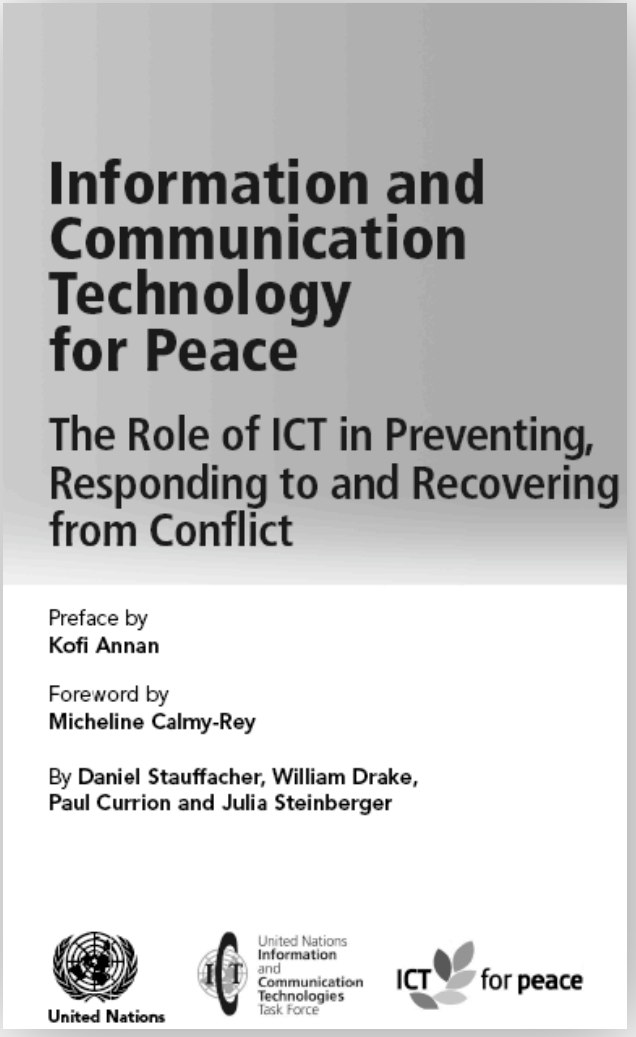
The Government of Kenya and ICT4Peace Foundation co-organize the first Regional Training Workshop in Africa on International Security and Diplomacy in Cyberspace

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

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."

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

Thank you very much

danielstauffacher@ict4peace.org