ICT for peace foundation

Building an International Governance for Peace and Security in Cyberspace

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

Certificate of Advanced Studies in Public Governance and Administration
ETH Zürich, 15 September 2017

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

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**

United Nations

United Nations
Information
and
Communication
Technologies
Task Force

ICT for peace

First Norm on ICT4Peace: 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.”

Ten Years later: Social media and internet technologies are used by almost half the world's population with adoption rising quickly

- Worldwide population: 7.5 billion
- The internet has 3.17 billion users
- 2.3m Google searches per minute (5 minutes downtime led to internet traffic drop of 40%; 6000 Tweets per second; 17 trillion webpages indexed by Google as of Jan 2016
- **2.3 billion active social media users (1.5bn on Facebook)**
- **Internet users have an average of 6 social media accounts.**
- **Social media users have risen by 200 million in the last year.**
- There are 1.65 billion active mobile social accounts globally with 1m more every day.

ICT for **peace** foundation

Source: Google, Mashable, Brandwatch

Modern communications technology bring significant advantages

- **Worldwide connectivity** and collaboration
- **Initially little or no regulation**, censorship, or government control (this situation changed rapidly)
- Potentially **huge audiences** spread throughout the world
- **Anonymity** of communication
- **Fast flow** of information for business and education
- **Inexpensive** development and maintenance of a web presence for all citizens and businesses
- The ability to **shape coverage in the traditional mass media**, which also increasingly uses the Internet as a source and audience for stories.

ICT for peace foundation

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 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.

September | 08

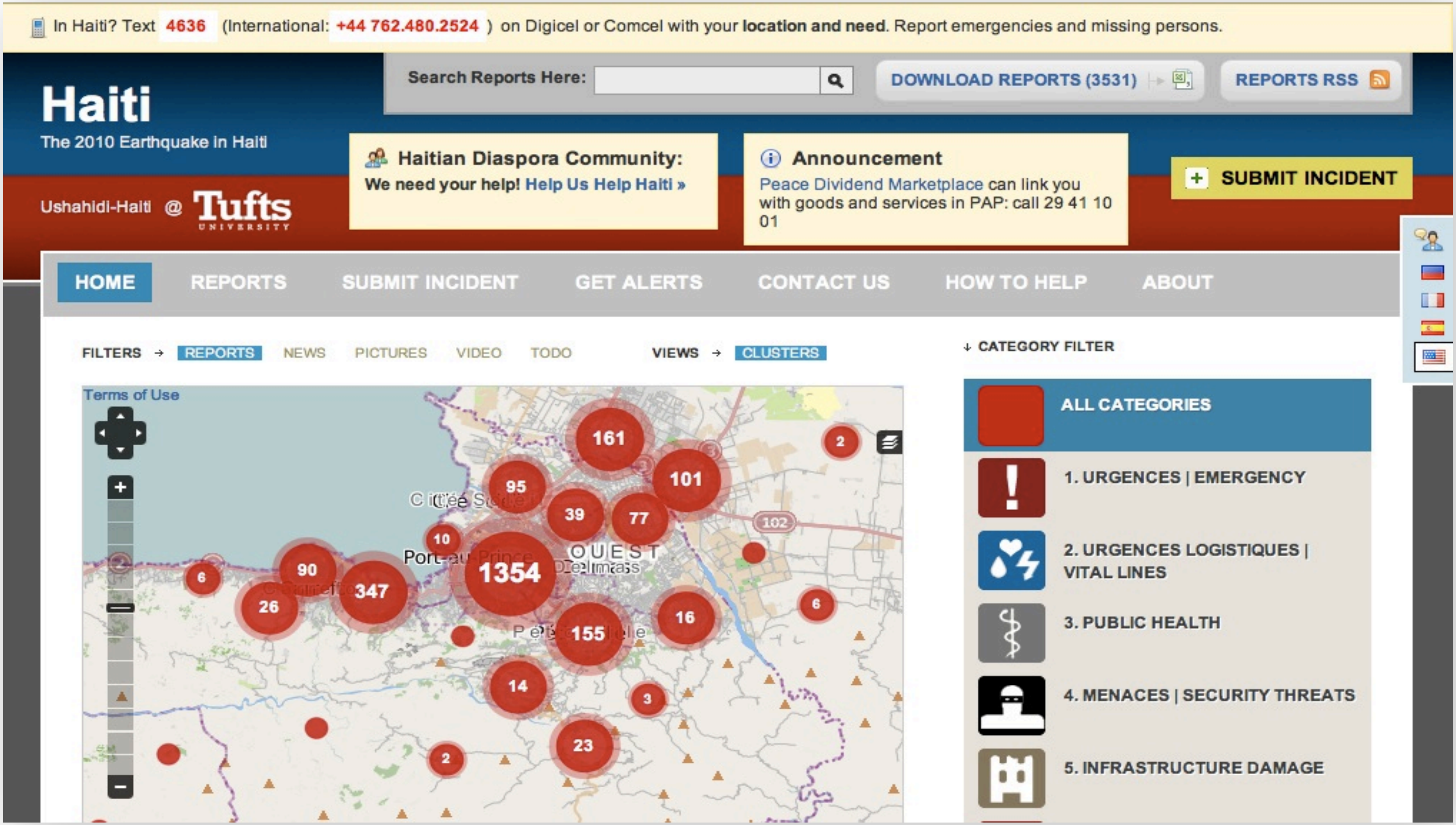
Interim Report: Stocktaking of UN Crisis Information Management Capabilities

Sanjana Hattotuwa and Daniel Stauffacher

ICT for peace foundation

UN Crisis Information Management Strategy for better decision Making : ONE UN, Combating Silos in Information Management and

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



In Haiti? Text **4636** (International: **+44 762.480.2524**) on Digicel or Comcel with your **location and need**. Report emergencies and missing persons.

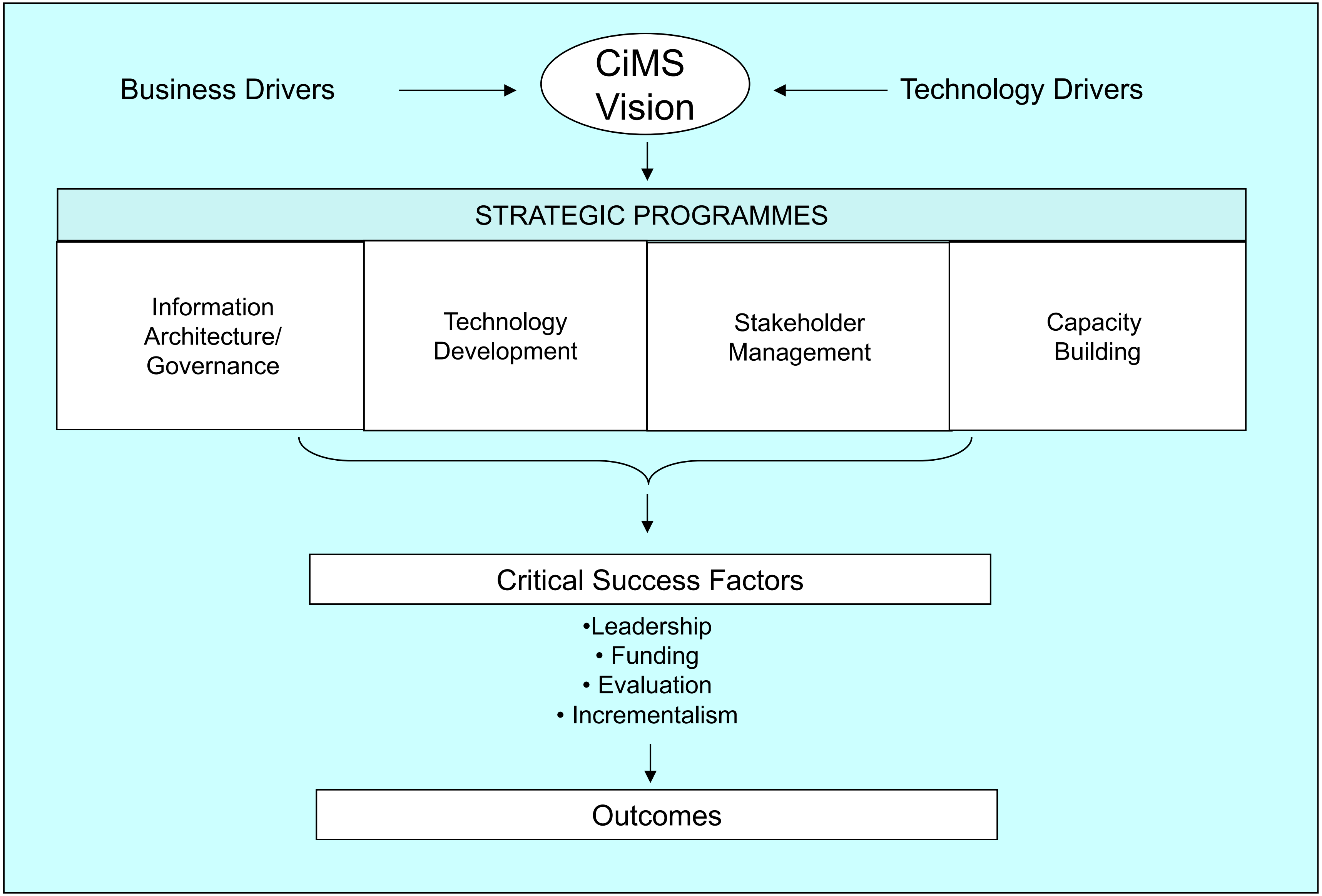
Haiti

The 2010 Earthquake in Haiti

Ushahidi-Haiti @ Tufts University

Haitian Diaspora Community:
We need your help! Help Us Help Haiti »

Announcement
Peace Dividend Marketplace can link you with goods and services in PAP: call 29 41 10 01



Business Drivers

CiMS Vision

Technology Drivers

STRATEGIC PROGRAMMES

Information Architecture/ Governance

Technology Development

Stakeholder Management

Capacity Building

Critical Success Factors

•Leadership

• Funding

• Evaluation

• Incrementalism

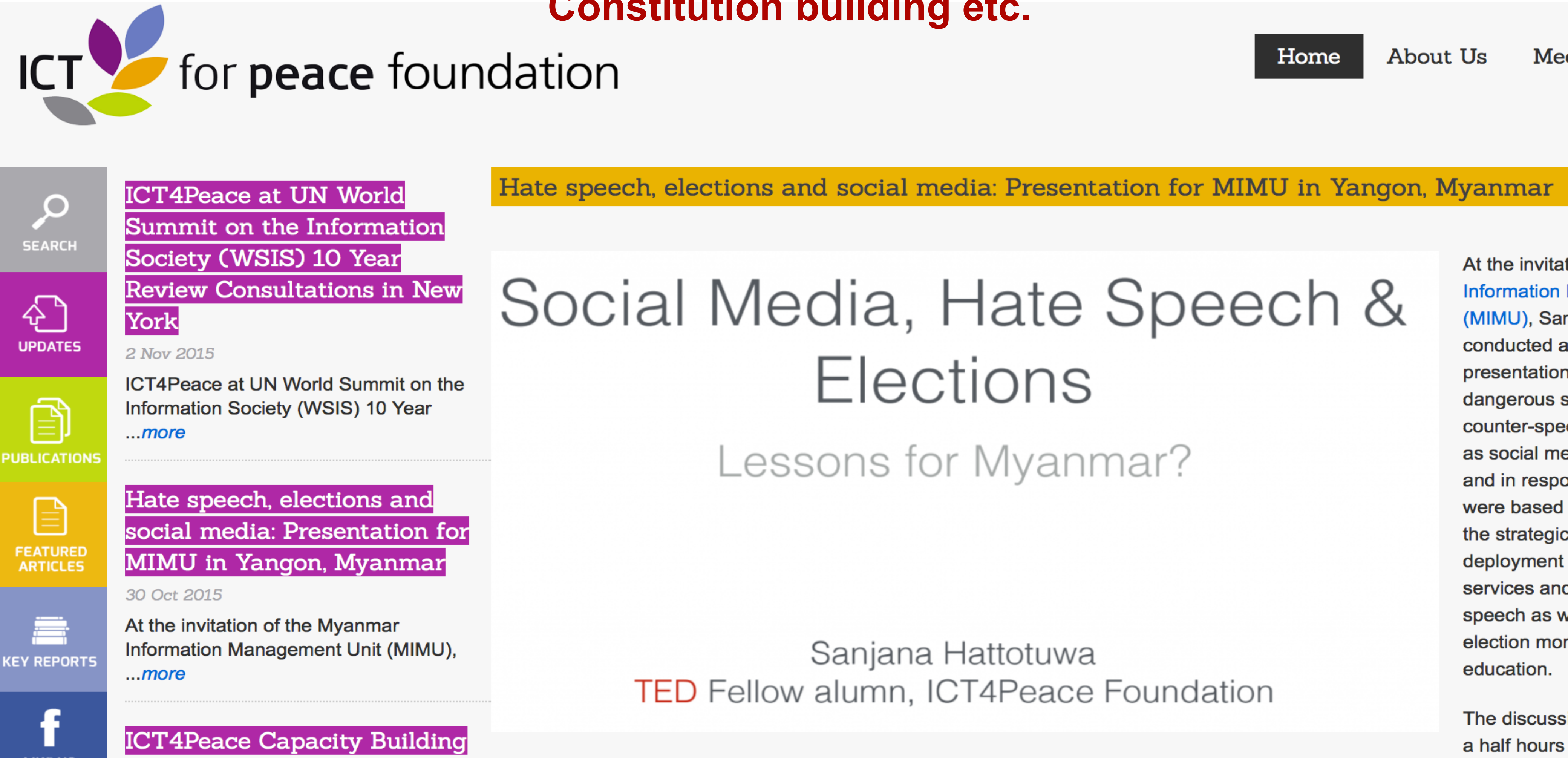
Outcomes

ICT for peace foundation

ICTs for the prevention of mass atrocity crimes

What is being done to support the prevention of mass atrocity crimes as well as reconciliation, healing and justice with a particular emphasis on the use of Information and Communications Technologies (ICTs)?

Examples of further ICT4Peace work, including Using ICTs for election monitoring, Constitution building etc.



ICT4Peace at UN World Summit on the Information Society (WSIS) 10 Year Review Consultations in New York

2 Nov 2015

ICT4Peace at UN World Summit on the Information Society (WSIS) 10 Year ...*more*

Hate speech, elections and social media: Presentation for MIMU in Yangon, Myanmar

30 Oct 2015

At the invitation of the Myanmar Information Management Unit (MIMU), ...*more*

ICT4Peace Capacity Building

Hate speech, elections and social media: Presentation for MIMU in Yangon, Myanmar

Social Media, Hate Speech & Elections

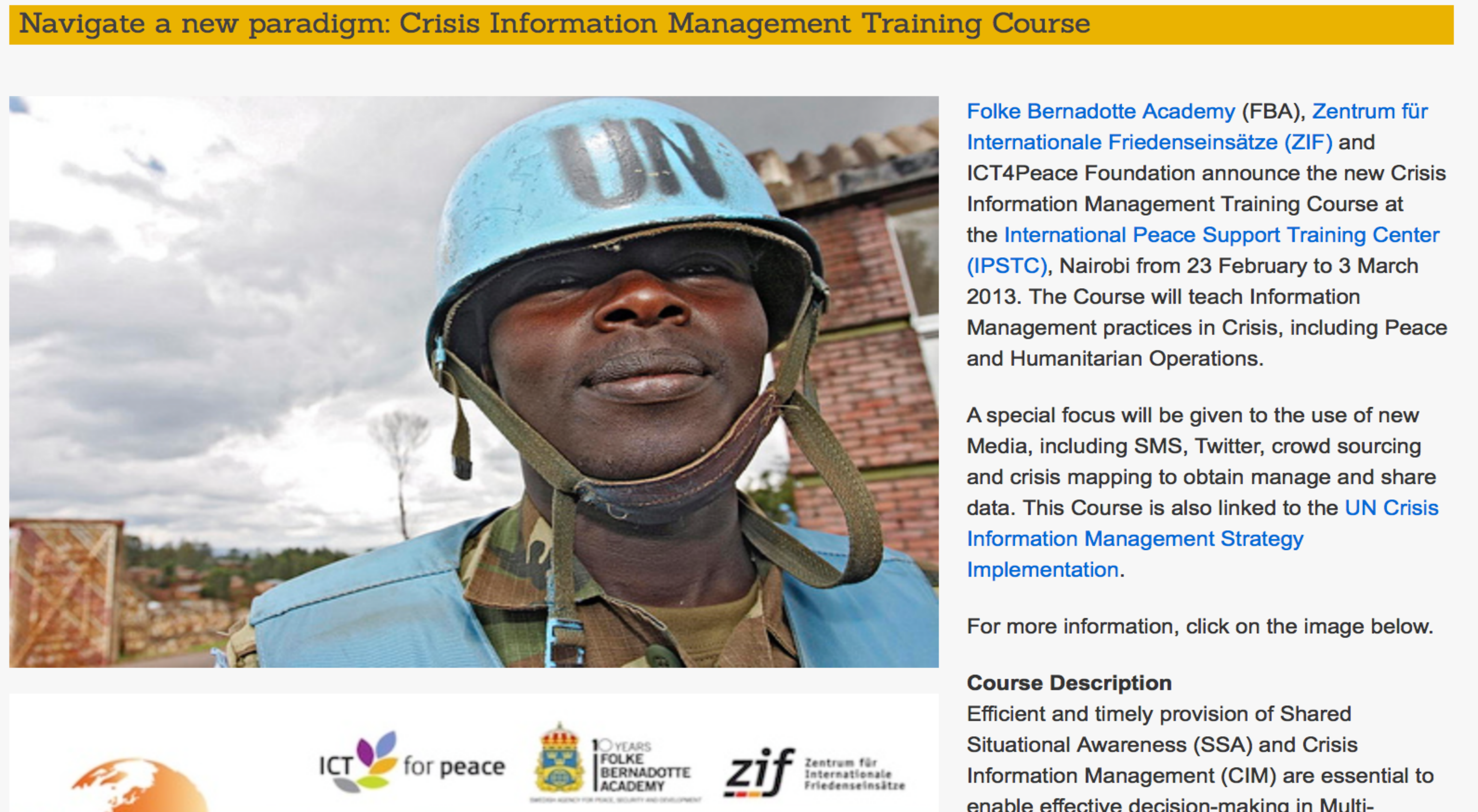
Lessons for Myanmar?

Sanjana Hattotuwa
TED Fellow alumn, ICT4Peace Foundation

At the invitat
Information
(MIMU), Sar
conducted a
presentation
dangerous s
counter-spe
as social me
and in respo
were based
the strategic
deployment
services and
speech as w
election mor
education.

The discuss
a half hours

Training Courses for better Crisis Information Management using ICTs and big data, social and new media,


ICT for peace
10 YEARS FOLKE BERNADOTTE ACADEMY
zif Zentrum für Internationale Friedenseinsätze

Navigate a new paradigm: Crisis Information Management Training Course

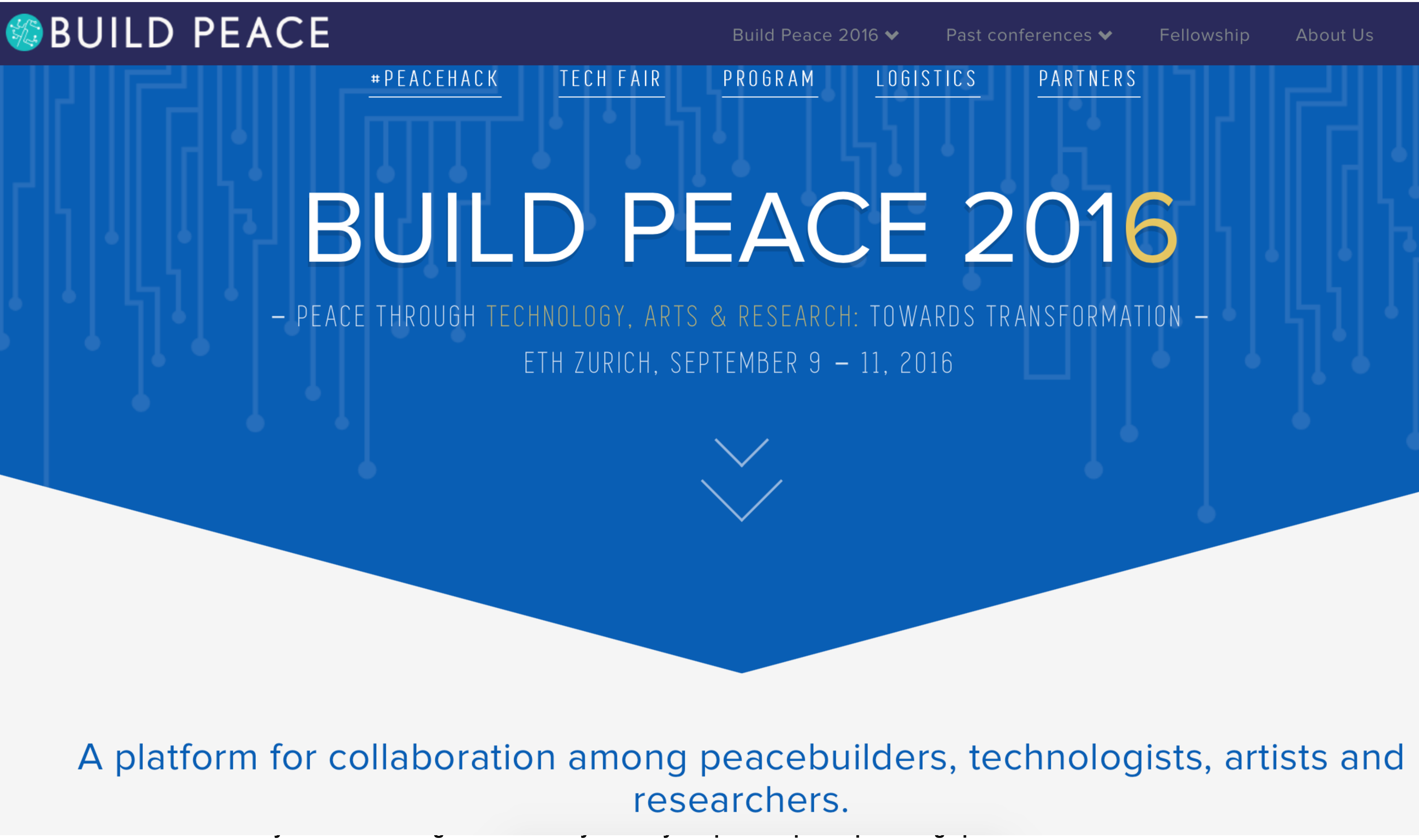
Folke Bernadotte Academy (FBA), Zentrum für Internationale Friedenseinsätze (ZIF) and ICT4Peace Foundation announce the new Crisis Information Management Training Course at the International Peace Support Training Center (IPSTC), Nairobi from 23 February to 3 March 2013. The Course will teach Information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

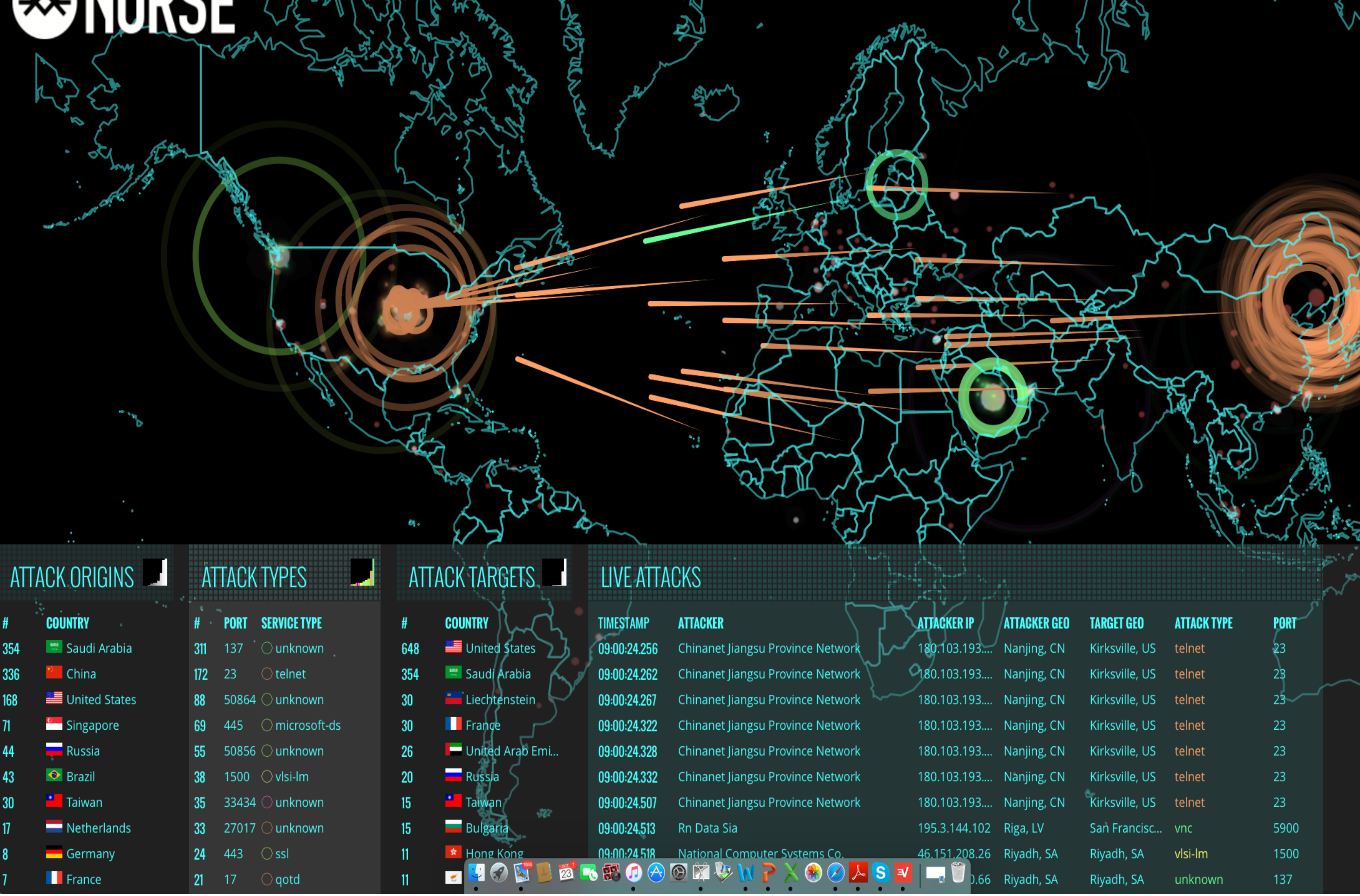


BUILD PEACE 2016

– PEACE THROUGH TECHNOLOGY, ARTS & RESEARCH: TOWARDS TRANSFORMATION –

ETH ZURICH, SEPTEMBER 9 – 11, 2016

A platform for collaboration among peacebuilders, technologists, artists and researchers.



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
		0.66	Riyadh, SA	Riyadh, SA	unknown	137

http://map.norsecorp.com/#/

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

- 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

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.**

The Cyber Security Challenge: What Can be Done ?

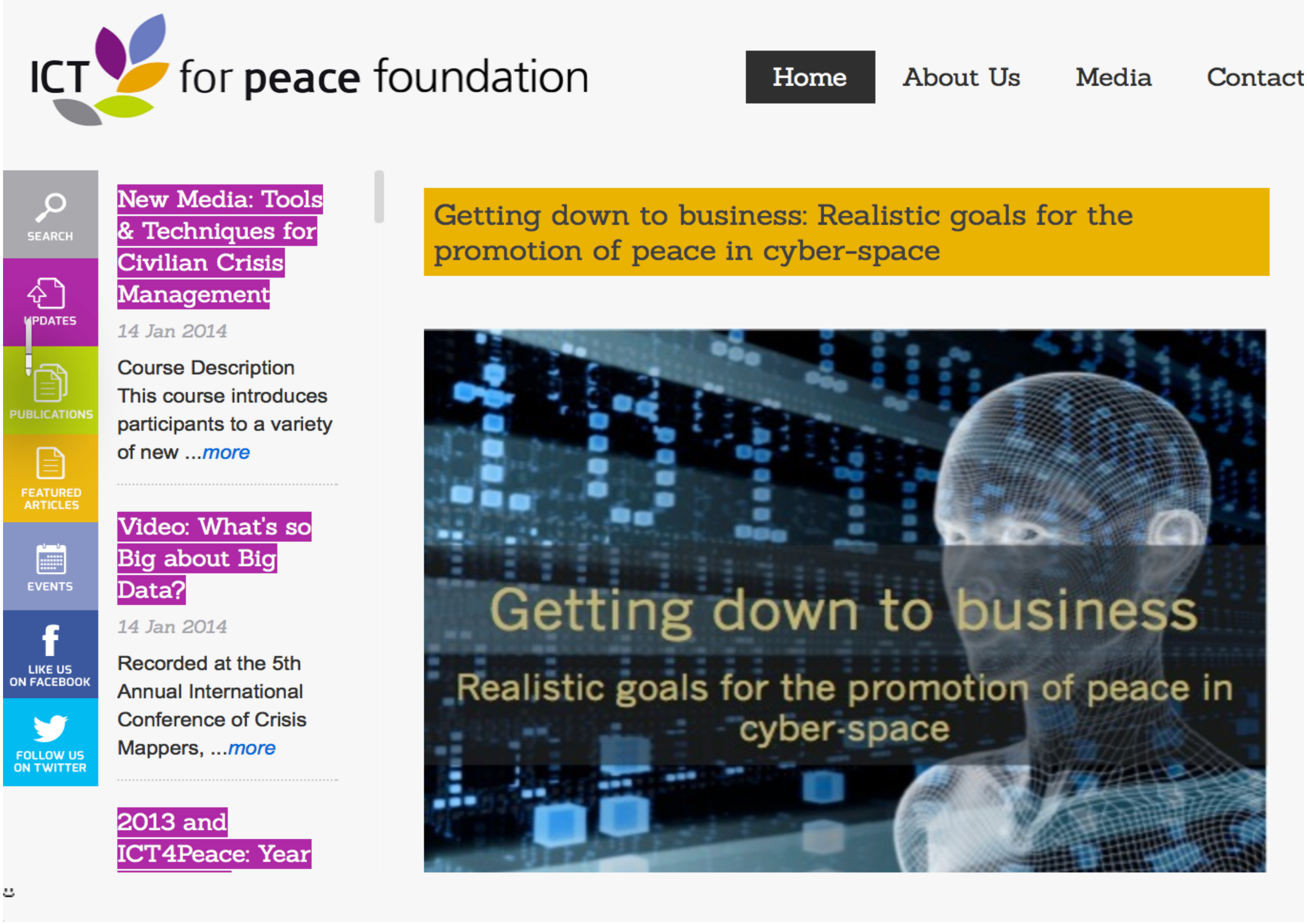
- These scenarios show that we need:

-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**



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.

ICT4Peace Policy Research and Advocacy on Peace, Trust and Security in Cyberspace

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

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

CYBER POLICY PROCESS BRIEF

AMBASSADOR (RET.) DANIEL STAUFFACHER, EDITOR
CAMINO KAVANAGH, RAPPORTEUR

CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY

GENEVA 2013
ICT4PEACE FOUNDATION

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’.

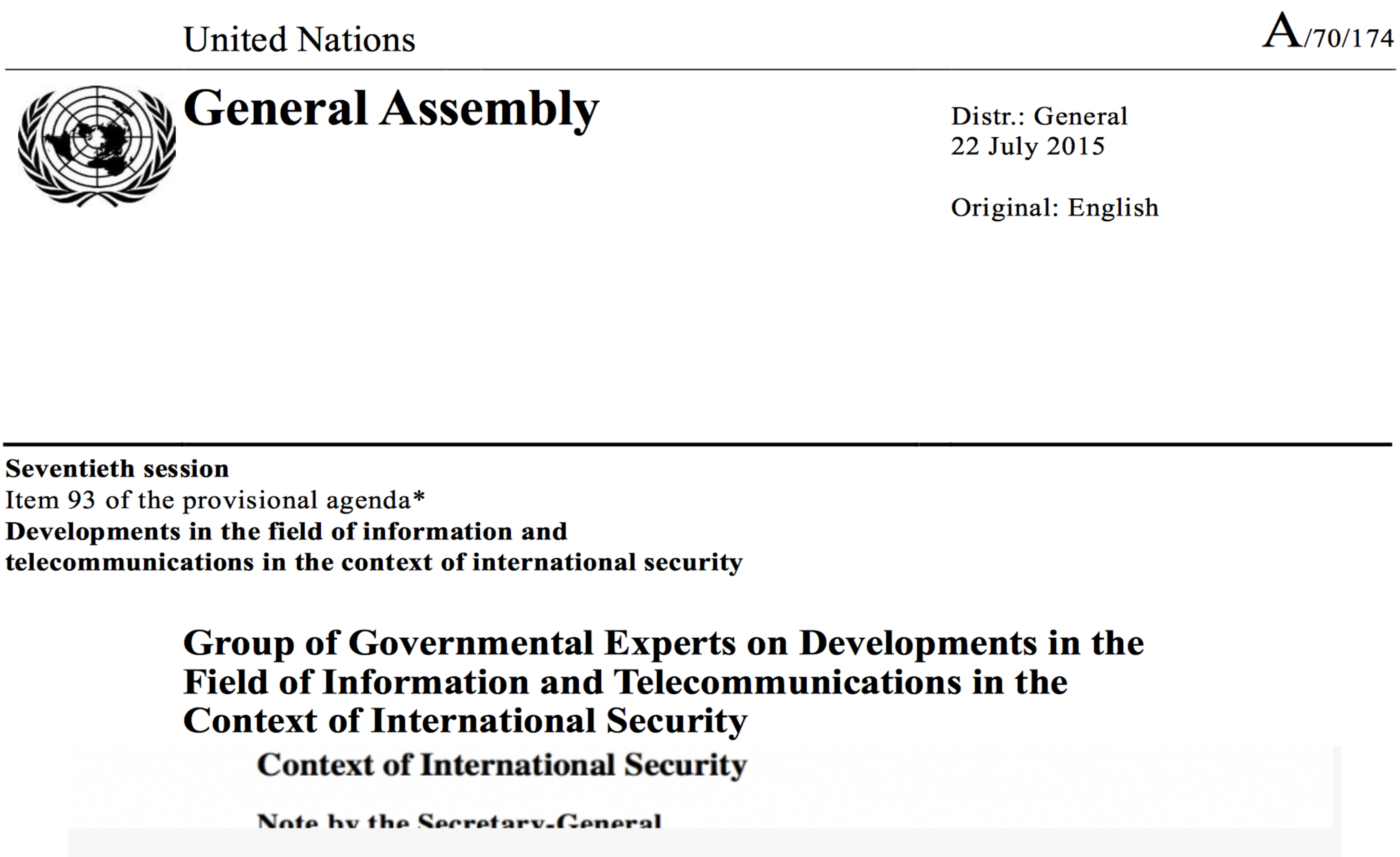
- A State should not conduct or knowingly support ICT that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public

- 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.

Confidence Building in Cyberspace: Constructive work by UN experts



United Nations

A/70/174

General Assembly

Distr.: General
22 July 2015

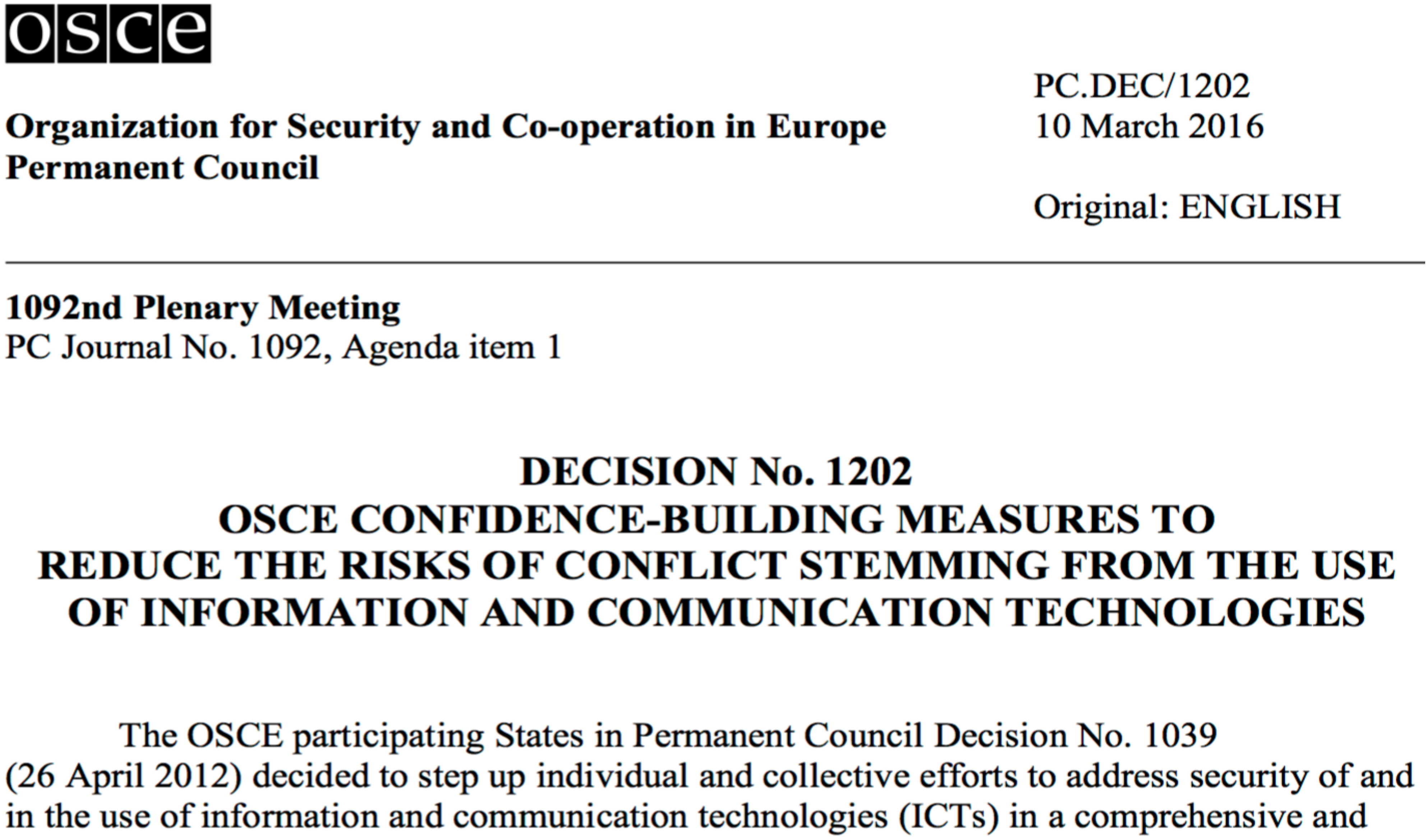
Original: English

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

Context of International Security

Note by the Secretary-General



osce

PC.DEC/1202
10 March 2016

Organization for Security and Co-operation in Europe
Permanent Council

Original: ENGLISH

1092nd Plenary Meeting
PC Journal No. 1092, Agenda item 1

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;

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. High Commissioner on Human Rights 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”.

- 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

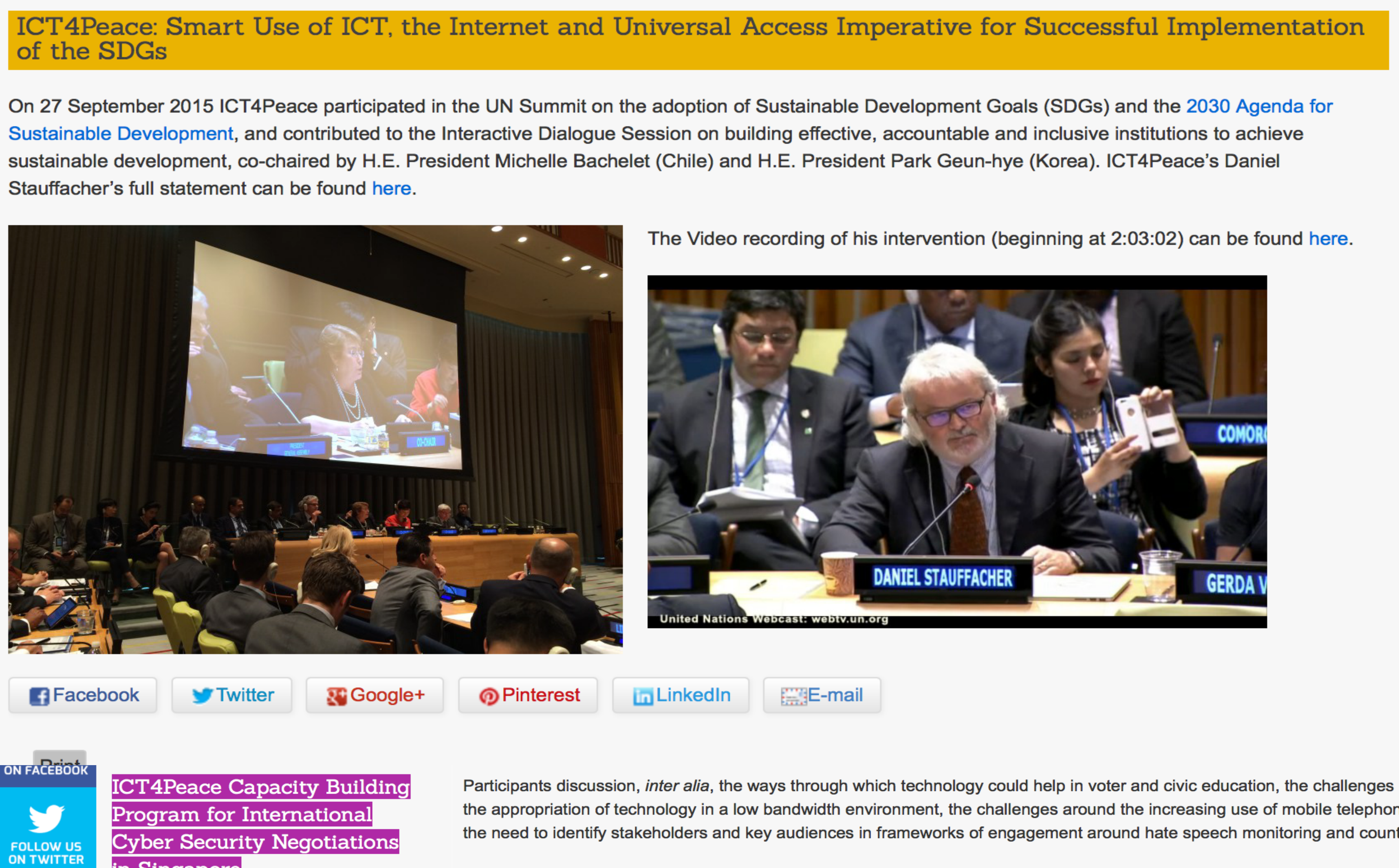
- The General Assembly can ill afford to have two deliberative streams (i.e. the First and Third Committee) acting in ignorance of one another.

Other Global Processes

- A review process of WSIS plus 10, including the security-related sections of the Geneva and Tunis Declaration of Principles, Plan of Action and Commitmentand was completed the UN General Assembly in December 2015.

- Sustainable Development Goals (SDGs) approved in December 2015

ICT4Peace at SDG Summit in New York



ICT4Peace: Smart Use of ICT, the Internet and Universal Access Imperative for Successful Implementation of the SDGs

On 27 September 2015 ICT4Peace participated in the UN Summit on the adoption of Sustainable Development Goals (SDGs) and the 2030 Agenda for Sustainable Development, and contributed to the Interactive Dialogue Session on building effective, accountable and inclusive institutions to achieve sustainable development, co-chaired by H.E. President Michelle Bachelet (Chile) and H.E. President Park Geun-hye (Korea). ICT4Peace's Daniel Stauffacher's full statement can be found here.

The Video recording of his intervention (beginning at 2:03:02) can be found here.

ICT4Peace Capacity Building Program for International Cyber Security Negotiations in Singapore

Participants discussion, *inter alia*, the ways through which technology could help in voter and civic education, the challenges the appropriation of technology in a low bandwidth environment, the challenges around the increasing use of mobile telephon the need to identify stakeholders and key audiences in frameworks of engagement around hate speech monitoring and count

Critique: UN Millenium Declaration vs UN SDGs vs WSIS plus 10

- The UN Millenium Declaration clearly stipulated that that Development cannot be achieved without peace and security, and peace and security cannot be maintained without development and well being of all.

- Unfortunately the UN Sustainable Development Goals (SDGs) approved by the World Leaders in 2015 do not contain clear and strong references to the need of Peace and Security.

- Similarly, WSIS plus 10 does not contain clear and strong language on the need for peace and security. It does make references to the UN GGE process on Cybersecurity.

Other Regional and Bilateral Processes: ASEAN REGIONAL FORUM (ARF)

- The **ASEAN Regional Forum (ARF), in its broader efforts on terrorism and transnational crime, has evolved into a regional platform in Asia for discussion among states on international cyber security issues.**

- E.g. **A 2012 workshop focused on proxy actors or 'groups and individuals, who on behalf of a state, take malicious cyber actions against the governments, the private sector and citizens of other states.**

- **Another workshop in September 2012 on confidence building** measures focused *inter alia,* on **'whether there is a lack of a cyber security legal framework' and how to build norms that reflect unacceptable action by states.**

- **In October 2013, the ARF hold a workshop on cyber security entitled 'Measures to Enhance Cyber Security—Legal and Cultural Aspects**' and **throughout that year, the ARF served as a platform for bilateral discussions with China and Japan as well as the U.S. on cyber security confidence building measures (CBMs).**

- **In 2014 and 2015, further ARF workshops were held towards reaching common ground on <u>specific cyber security-related confidence building measures (CBMs) for the Asia-Pacific region.</u>**

ORGANISATION OF AMERICAN STATES (OAS)

- **Since the early 2000s cyber security has featured on the OAS working agenda** and **was the first region of the world to develop a strategy to counter threats to cyber security.**

- **Yet this focus has centered mainly on ensuring a common framework for dealing with cybercrime and other forms of organized crime,** ensuring **that states have the relevant capacity to respond to system vulnerabilities, and ensuring that state responses are also aligned with OAS efforts to strengthen democratic governance and the regional human rights architecture.**

- **In 2014 the OAS in cooperation with ICT4Peace held the first Cyber Security Policy and Diplomacy Course for 24 countries in Bogota, discussing for the first time concepts such as norms of responsible state behaviour and Confidence Building Measures (CBMs) for the cyber space.**

SHANGHAI COOPERATION ORGANISATION (SCO), COLLECTIVE SECURITY TREATY ORGANISATION (CSTO) AND COMMONWEALTH OF INDEPENDENT STATES (CIS)

- **In September 2011, a group of countries led by the Russian Federation and the People's Republic of China** proposed an **'International Code of Conduct for Information Security'** for consideration at the **66th session of the UN General Assembly**.

- **In 2011, the Russian Federation** released a **'concept for a Convention on International Information Security'** at the second International Meeting of High-Ranking Officials Responsible for Security Matters in Yekaterinburg, Russia in 2011.

- **Both the Code of Conduct and the draft Convention include voluntary provisions banning the use of the Internet for military purposes** and for the overthrow of regimes in other countries.

- **The Code of Conduct and Concept for an International Convention on Information Security are supported by the Shanghai Cooperation Organization (SCO), the Collective Security Treaty Organisation (CSTO) and the Commonwealth of Independent States (CIS).**

AFRICAN UNION

- **So far cybercrime has been identified as a core concern for Africa** and efforts are underway to develop a common cyber security strategy for the region.

- In 2014 the African Union adopted the **African Union Convention on Cyber Security and Data Protection, which** covers a wide range of online activities, **including electronic commerce, data protection, and cybercrime, with a special focus on racism, xenophobia, child pornography, and national cybersecurity**. When implemented, many African nations will enact personal data protection laws for the first time, and upheld by new, independent public authorities.

- **In early 2015 the Government of Kenya in cooperation with ICT4Peace held the first Cyber Security Policy and Diplomacy Course for 12 East African countries in Nairobi, discussing Norms of Responsible State Behaviour and Confidence Building Measures (CBMs) for the Cyberspace.**

NORTH ATLANTIC TREATY ORGANISATION (NATO)

- In 2013, **the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)**, **an independent think tank accredited by NATO, released the ‘Tallinn Manual on the International Law Applicable to Cyberspace.’**

- **Written at the invitation of the CCD COE by 20 legal scholars and practitioners, the Tallinn Manual explores the applicability of international humanitarian law and the doctrines of *jus ad bellum* to cyber conflicts, and offers a range of definitions, including a definition of the much disputed term of what constitutes a ‘cyber attack.’**

- **This exercise demonstrated the challenge of interpreting international law norms in the cyber context. The Tallinn Manual has, however, advanced the discussion of how international law might apply in and to cyberspace.**

EUROPEAN UNION

- In **February 2013, the European Union adopted a cyber security strategy, which focuses principally on ensuring an open Internet, responding more effectively to cybercrime and protecting critical infrastructure.**

- As noted in a recent study**, other initiatives within the regional organisation's Common Foreign and Security Policy (CFSP) pillar are less developed**, although the **region's 2008 Security Strategy included 'cyber threats' as a new category of risks to European Security.**

- The **European Defence Agency (EDA)** and the **EU Military Council (EMC)** have been **working on different aspects of computer network operations (CNO) since 2008** and a **series of research exercises in the field of common defence and seminars have since been held on cyber security and implications for European CFSP.**

BILATERAL EFFORTS IN THE FIELD OF INTERNATIONAL AND REGIONAL SECURITY

- **At the bilateral level, several track 1, 1.5 and track 2 dialogues have been taking place between states and other relevant stakeholders on international and regional cyber security issues.**

- **These initiatives are aimed largely at building better understanding, trust and confidence between the parties and establishing joint mechanisms to avoid escalation to armed conflict**.

- **Track 1 policy dialogues (among states) include the processes between China and the U.S. within the framework of their on-going strategic dialogue, as well as between China and the UK, China and Germany, and China and Europe; between Germany and the U.S., and Germany and India; between Russia and India, and Russia and Brazil.**

- **On its part, the U.S. is engaged in bilateral discussions with Japan, India, Brazil, Russia, South Africa and South Korea. Meanwhile, ASEAN is hosting discussions with Japan, China and the U.S**.

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

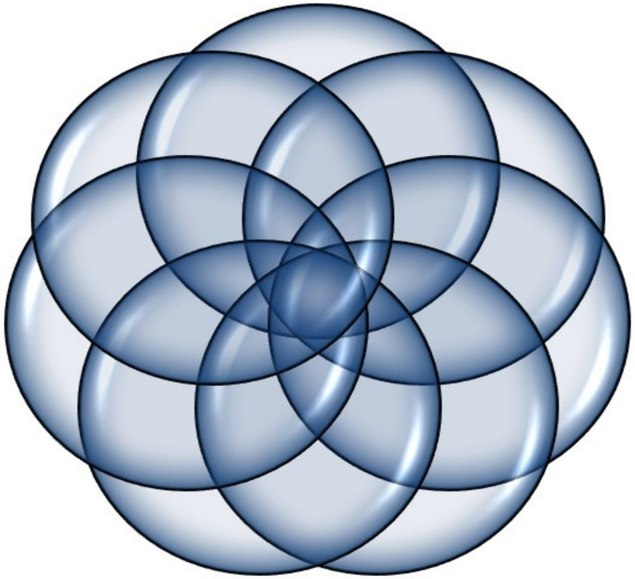
UNITED STATES
- Brazil
- China
- India
- Japan
- Russia
- Sth. Korea

UNITED KINGDOM
- China
- India

SOUTH KOREA
- US
- India

RUSSIA
- US
- India
- Brazil

BRAZIL
- Russia
- US

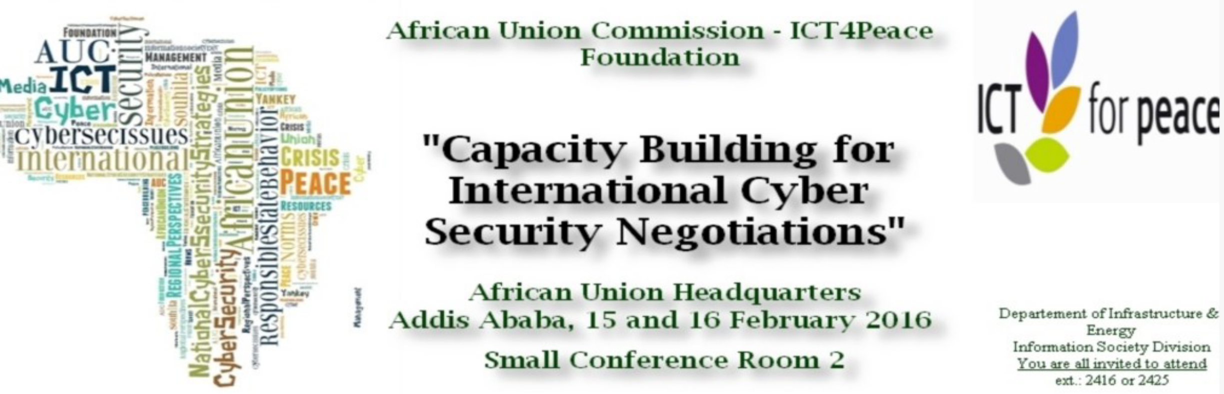


CHINA
- UK
- US
- EU
- Germany

GERMANY
- US
- India
- China

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

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


AUC
ICT
Media
Cyber
cybersecissues
international
security
Africanunion
CRISIS
PEACE
ICT for peace

African Union Commission - ICT4Peace Foundation

"Capacity Building for International Cyber Security Negotiations"

African Union Headquarters
Addis Ababa, 15 and 16 February 2016

Small Conference Room 2

Departement of Infrastructure & Energy
Information Society Division
You are all invited to attend
ext.: 2416 or 2425

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

Promoting Norms of Responsible Behaviour in Cyberspace

ASEAN CYBER NORMS WORKSHOP
8 - 9 MAY 2017
SINGAPORE

Organised by:
CSA SINGAPORE

As an initiative under:
ACCP
ASEAN Cyber Capacity Programme

In collaboration with:
ICT for peace foundation

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 fourty 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.

ICT4Peace briefs the UN Security Council on Peace and Security in Cyberspace (New York 28 November 2016)

tech
against
terrorism

Connecting industry, government, and civil society to prevent
the terrorist use of the internet whilst respecting human rights

tech_against_***terrorism***_.org_   *@techvsterrorism*

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

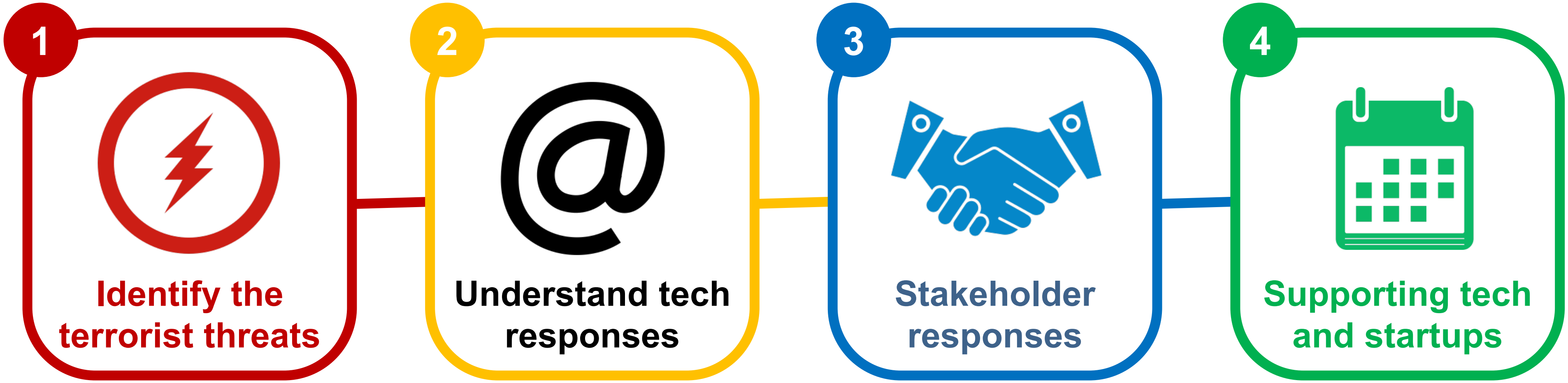
ICT for peace foundation

UN CTED
Counter-Terrorism Committee
Executive Directorate

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

2 Understand tech responses

3 Stakeholder responses

4 Supporting tech and startups

- How are terrorists exploiting tech?
- What are the most important areas to consider our work?

- How are tech companies responding?
- What are the strengths and weaknesses?
- What can we learn?

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

- What can we do to provide operational support to tech and startups?
- How can we inform States about the best approaches?

ICT for peace foundation

We held workshops in Zurich, Silicon Valley, and Kuala Lumpur

Zurich
Kuala Lumpur
Silicon Valley

In this project we are focusing on tech organisations that can be exploited by terrorists to publicise, recruit, and support operations

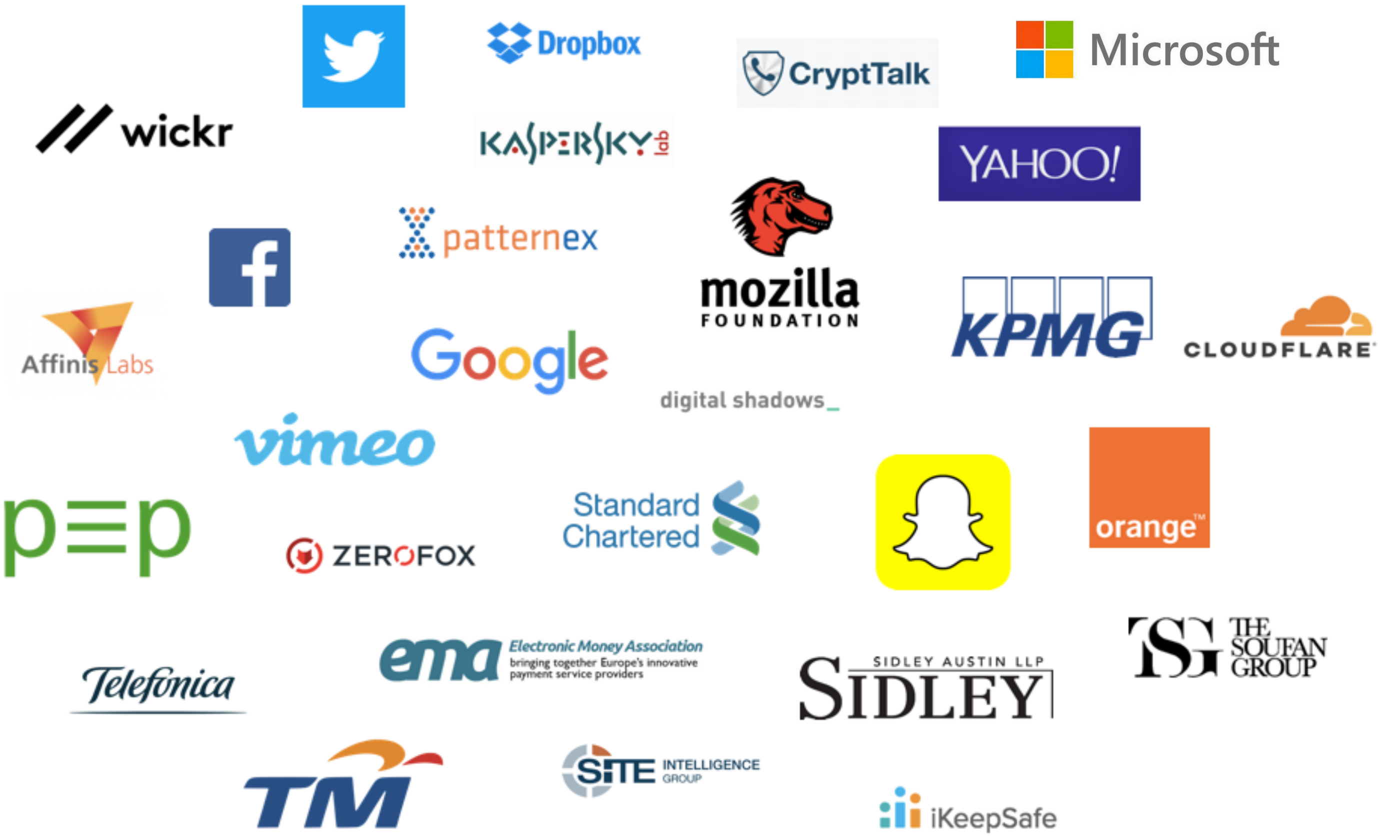
1 Publicity and recruitment

- Social media and sharing platforms
- Content storage and knowledge sharing

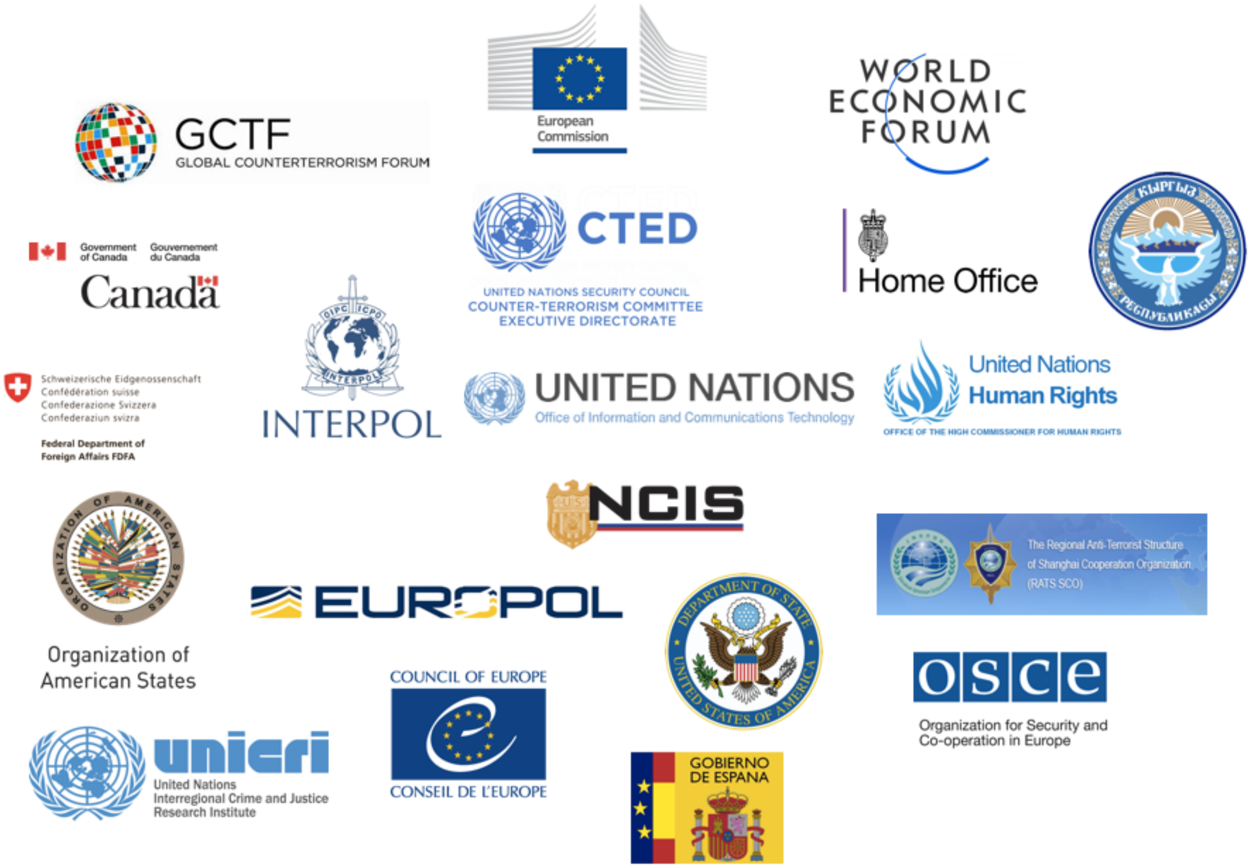
2 Operational usage (overt / covert)

- Communications and messaging
- Financial funding and transfers

ICT4Peace Global workshops included industry representatives from technology, media, telecommunications, and finance



ICT4Peace Global workshops included governments and inter-governmental organisations and agencies


GCTF
GLOBAL COUNTERTERRORISM FORUM
European Commission
WORLD ECONOMIC FORUM
Government of Canada
Gouvernement du Canada
Canada
CTED
UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE
Home Office
КЫРГЫЗ РЕСПУБЛИКАСЫ
INTERPOL
OIPC ICPO
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Federal Department of Foreign Affairs FDFA
UNITED NATIONS
Office of Information and Communications Technology
United Nations Human Rights
OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
NCIS
ORGANIZATION OF AMERICAN STATES
Organization of American States
EUROPOL
The Regional Anti-Terrorist Structure of Shanghai Cooperation Organization (RATS SCO)
DEPARTMENT OF STATE UNITED STATES OF AMERICA
osce
Organization for Security and Co-operation in Europe
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
unicri
United Nations Interregional Crime and Justice Research Institute
GOBIERNO DE ESPANA

ICT4Peace Global workshops included leading civil society organisations and human rights groups

ADL
Anti-Defamation League®

IPAC
INSTITUTE FOR POLICY ANALYSIS OF CONFLICT

EFF
ELECTRONIC FRONTIER FOUNDATION

SECDEV.FOUNDATION

GLOBAL NETWORK INITIATIVE

CPJ Committee to Protect Journalists
Defending Journalists Worldwide

ICCT International Centre for Counter-Terrorism - The Hague

cdt
CENTER FOR DEMOCRACY & TECHNOLOGY

OpenNet Initiative

VOX Pol

accessnow

FSM Freiwillige Selbstkontrolle Multimedia-Diensteanbieter

ICT4Peace Global workshops included academic institutions and think tanks who contributed papers for each of the meetings

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NANYANG TECHNOLOGICAL UNIVERSITY

DCU

ISIS MALAYSIA

SCHOOL OF LAW
UNIVERSITY *of* CALIFORNIA · IRVINE

BRENNAN CENTER FOR JUSTICE
at New York University School of Law

KING'S *College* LONDON

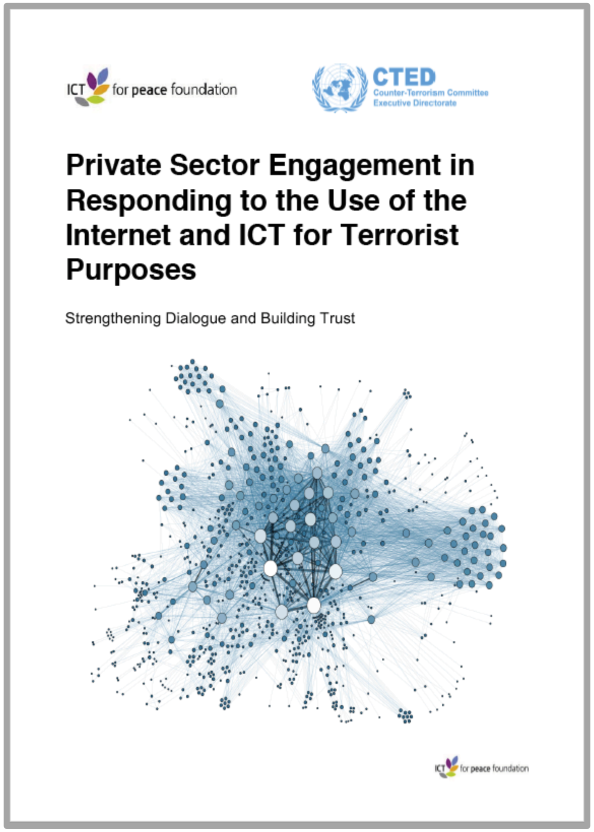
ETH Zürich

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

॥न्यायस्तत्र प्रमाण स्यात् ॥
NLU
DELHI

We presented our summary report for Phase 1 at the UN CTC in December 2016



ICT for peace foundation

CTED
Counter-Terrorism Committee
Executive Directorate

Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes

Strengthening Dialogue and Building Trust

ICT for peace foundation

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

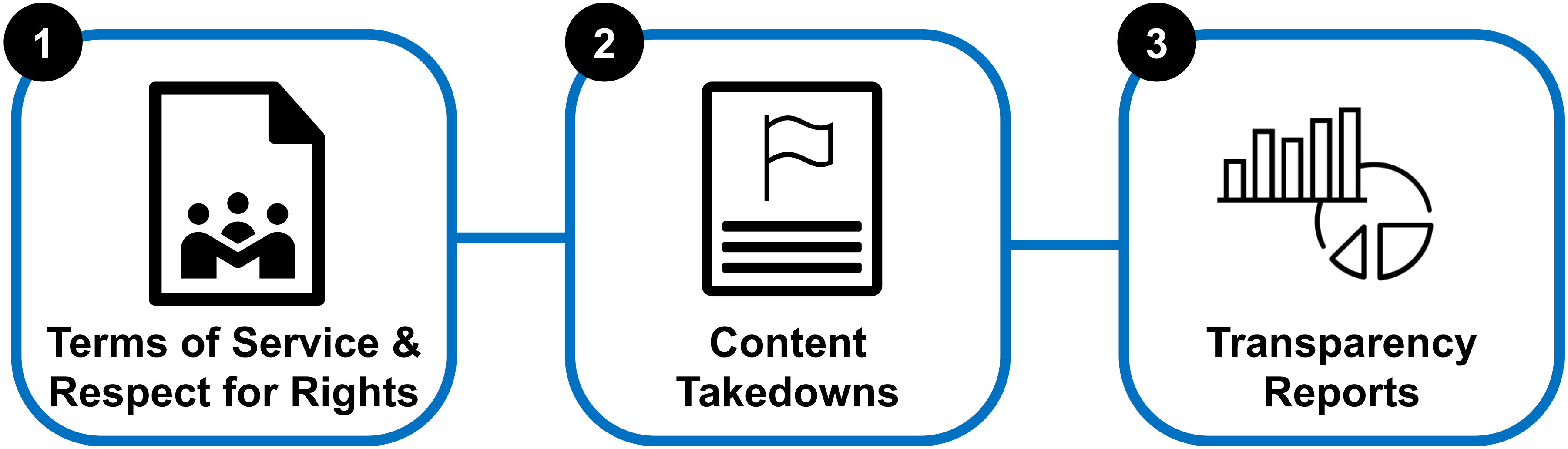
Respect for human rights

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

2 Content Takedowns

3 Transparency Reports

- Community guidelines and standards respecting freedom of expression and human rights principles
- Operational definitions of violent extremism and terrorism

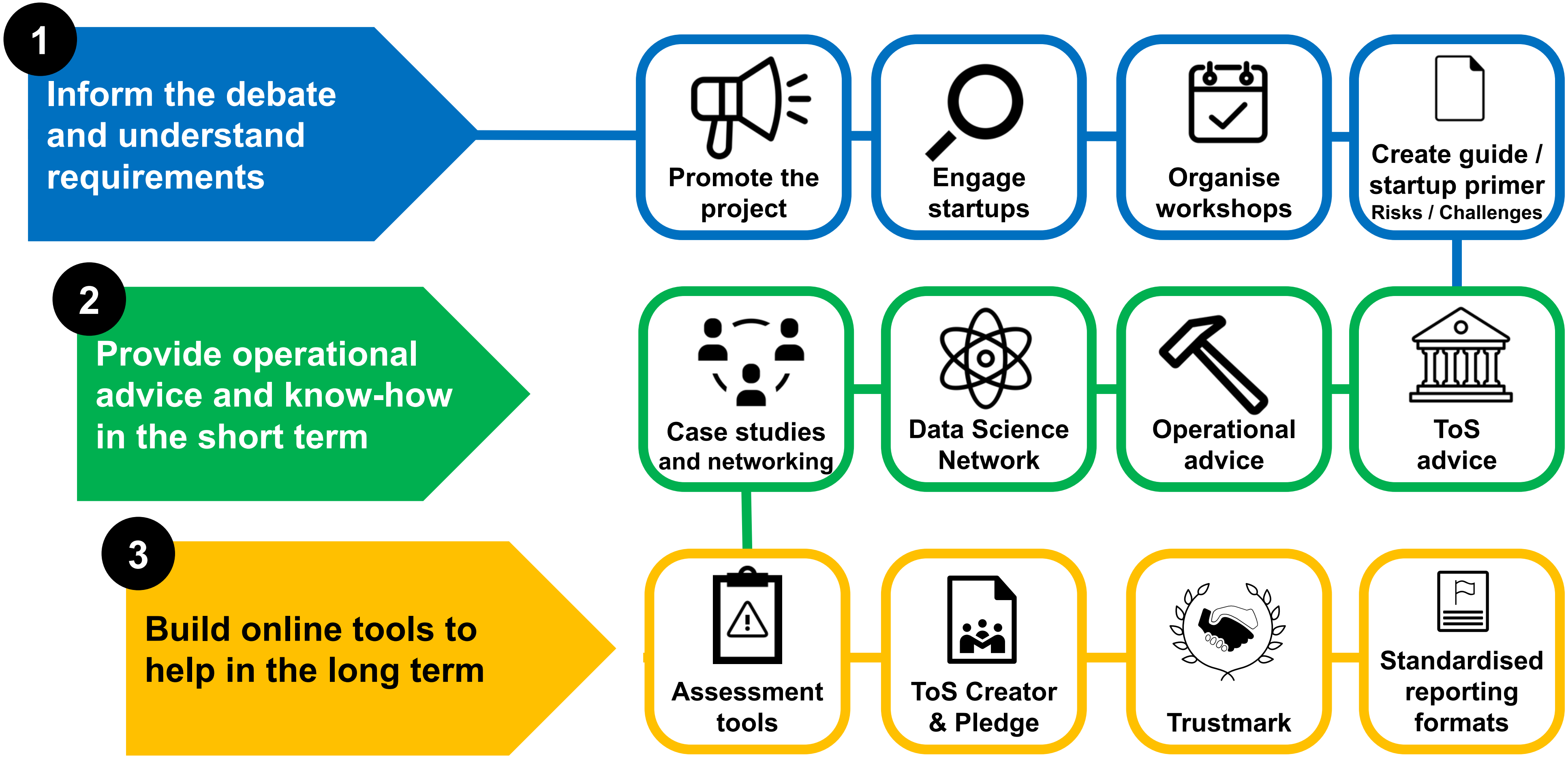
- Content reporting by users, NGOs, and governments
- Engagement with law enforcement
- Engagement with Internet Referral Units (IRUs)
- Careful deliberation of what content / accounts to take down given ToS

- Regular reports of government and user-generated take-down requests
- Transparency around government requests as protection against censorship concerns

ICT for peace foundation

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

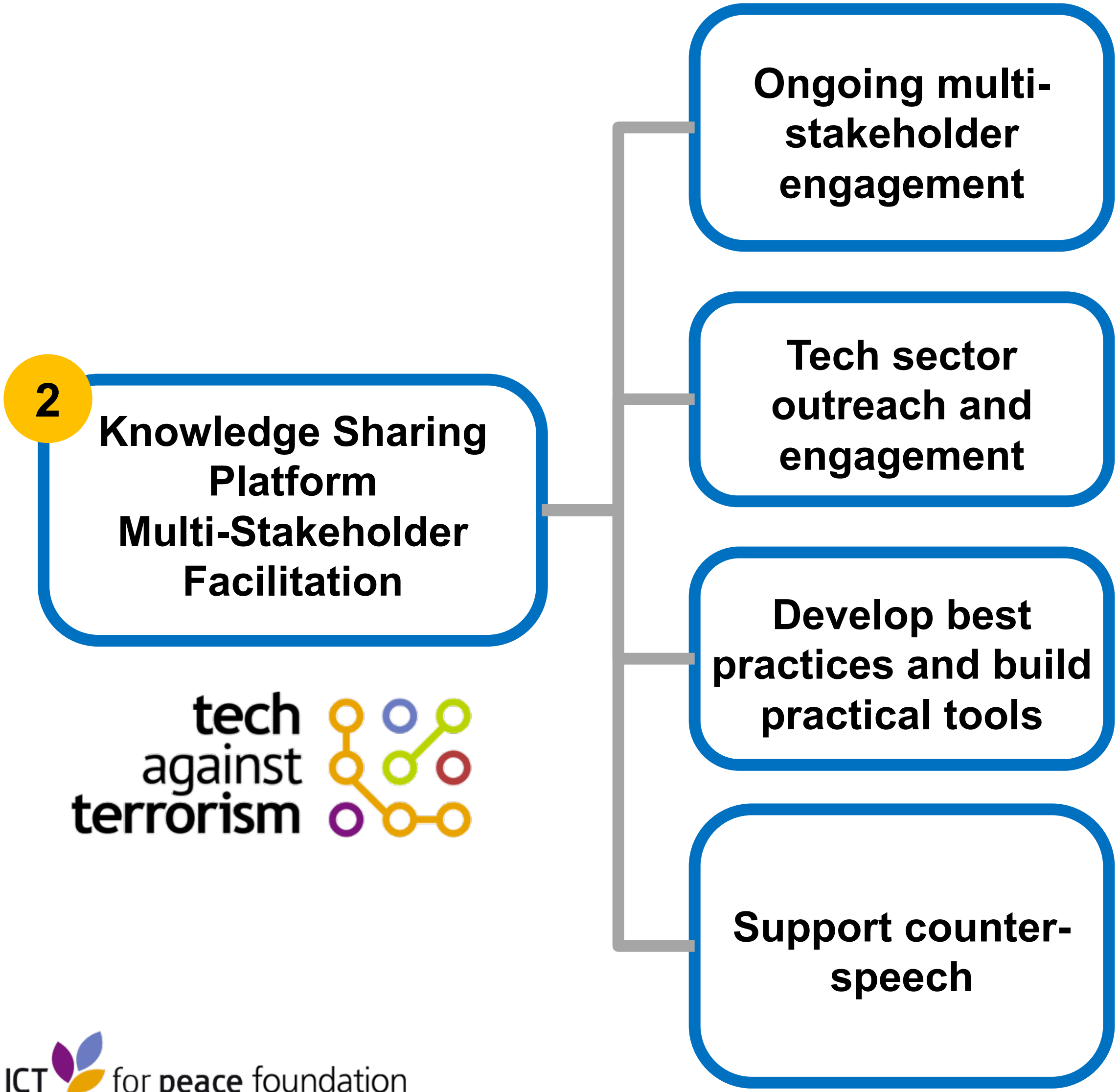
2 Provide operational advice and know-how in the short term

- 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

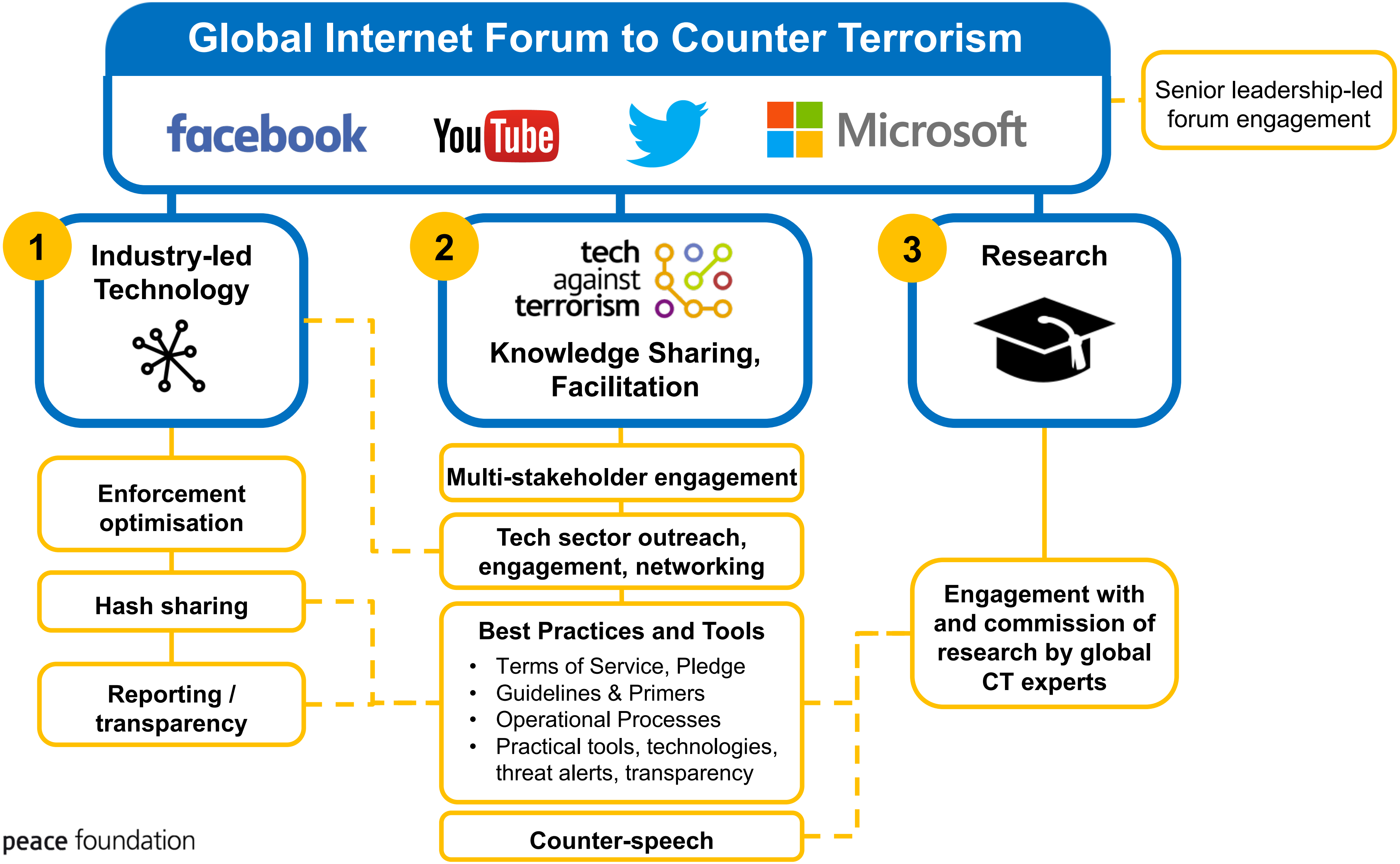
Support counter-speech

- Learn from counter-speech initiatives and further empower the tech industry and civil society to engage in this work

tech against terrorism

ICT for peace foundation

- **Tech Against Terrorism is supporting the GIFCT to facilitate knowledge-sharing and multi-stakeholder engagement**



Global Internet Forum to Counter Terrorism

Senior leadership-led forum engagement

1 Industry-led Technology

Enforcement optimisation

Hash sharing

Reporting / transparency

2 tech against terrorism

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

ICT for peace foundation

Merci Beaucoup

danielstauffacher@ict4peace.org

UN CTED
Counter-Terrorism Committee
Executive Directorate

ICT for peace foundation

Joint ICT4Peace and UN CTED project: *Private sector engagement in responding to the terrorist use of ICT*

Objectives of the joint ICT4Peace and UN CTED project

- **Deepen the knowledge base by identifying and assessing:**

  - Voluntary and non-voluntary measures adopted by the technology sector in response to terrorist use of their products and services.

  - The emerging discussion on the potential use of measures such as sanctions to respond to terrorist use of ICT

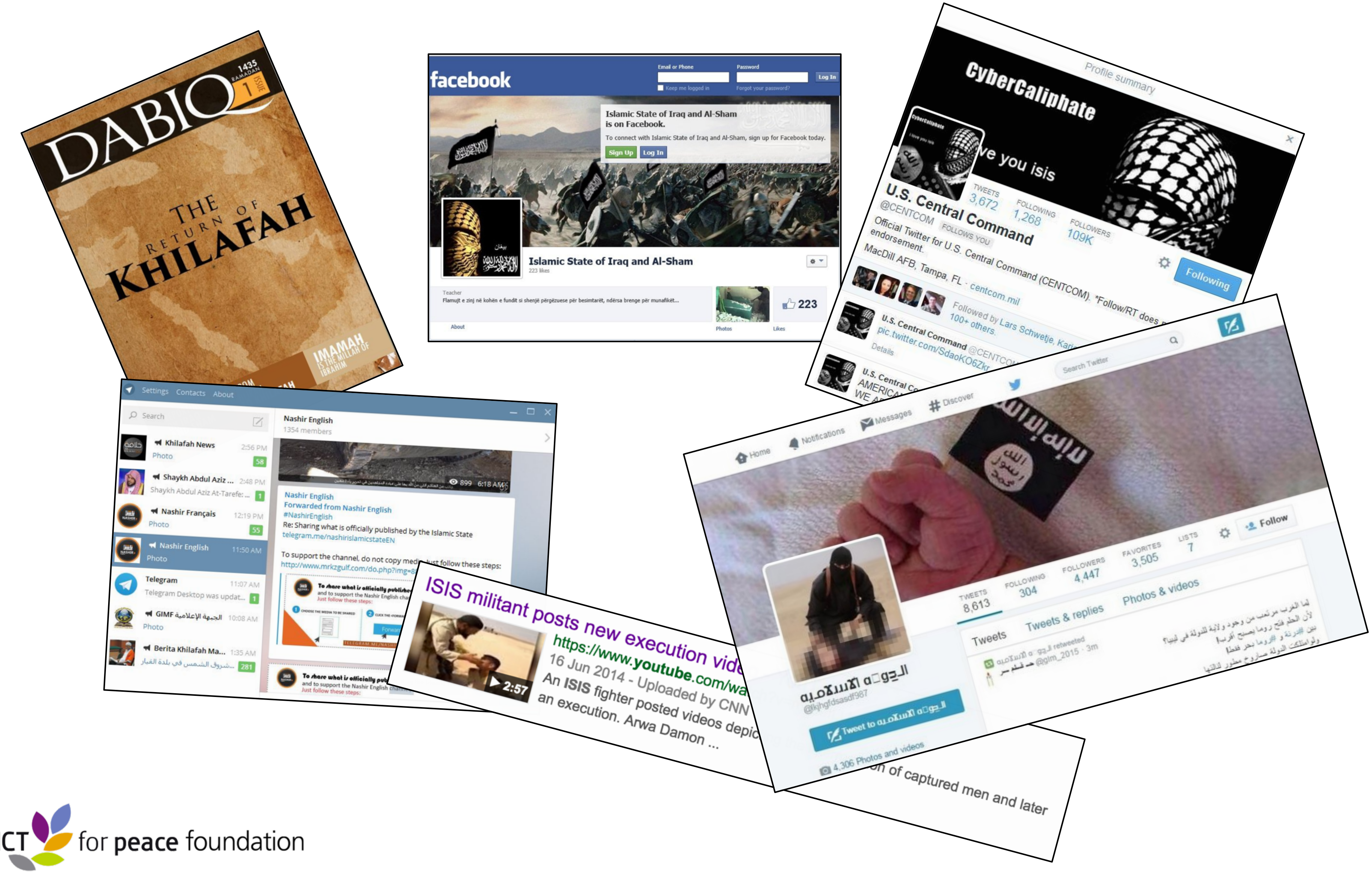
- **Work with industry players to establish a forum / online curated platform to share voluntary norms, principles, and practices**

As "technological entrepreneurs" some terrorists have taken advantage of ICT to promote their propaganda and support operations

Content / Propaganda

- Exploit **inherently decentralised and open nature of the internet and the freedom of expression it allows**
- Conduct **strategic communications promoting terrorists extremist causes**
- **Galvanise support** and **drive recruitment**
- **Harass and intimidate** the global internet population
- Attempt to **polarise society**
- **Aggravate existing societal tensions**

As well as creating its own content such as Dabiq, ISIS fully exploits technology platforms such as Facebook, Twitter, YouTube and Telegram



DABIQ
1435 RAMADAN
1 ISSUE
THE RETURN OF KHILAFAH
IMAMAH IS THE MILLAH OF IBRAHIM

facebook
Email or Phone
Password
Log In
Keep me logged in
Forgot your password?
Islamic State of Iraq and Al-Sham is on Facebook.
To connect with Islamic State of Iraq and Al-Sham, sign up for Facebook today.
Sign Up
Log In
Islamic State of Iraq and Al-Sham
223 likes
Teacher
Flamujt e zinj në kohën e fundit si shenjë përgëzuese për besimtarët, ndërsa brenge për munafikët...
223
About
Photos
Likes

Profile summary
CyberCaliphate
i love you isis
U.S. Central Command
@CENTCOM FOLLOWS YOU
TWEETS 3,672
FOLLOWING 1,268
FOLLOWERS 109K
Following
Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.
MacDill AFB, Tampa, FL · centcom.mil
Followed by Lars Schwetje, Kari… 100+ others.
U.S. Central Command @CENTCOM
pic.twitter.com/SdaoKO6Zkr
Details
U.S. Central C…
AMERICA…
WE A…

Settings Contacts About
Search
Khilafah News 2:56 PM
Photo 58
Shaykh Abdul Aziz ... 2:48 PM
Shaykh Abdul Aziz At-Tarefe: ... 1
Nashir Français 12:19 PM
Photo 55
Nashir English 11:50 AM
Photo
Telegram 11:07 AM
Telegram Desktop was updat... 1
GIMF الجبهة الإعلامية 10:08 AM
Photo
Berita Khilafah Ma... 1:35 AM
شروق الشمس في بلدة القيار... 281

Nashir English
1354 members
899 6:18 AM
Nashir English
Forwarded from Nashir English
#NashirEnglish
Re: Sharing what is officially published by the Islamic State
telegram.me/nashirislamicstateEN

To support the channel, do not copy medi… Just follow these steps:
http://www.mrkzgulf.com/do.php?img=8…

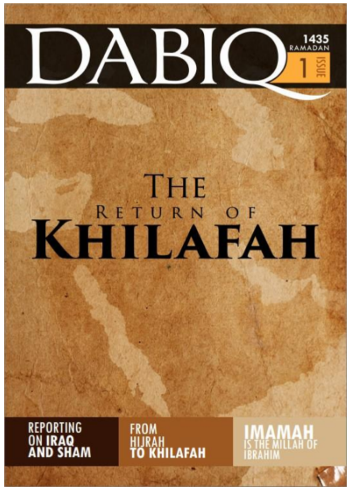
To share what is officially publishe… and to support the Nashir English cha… Just follow these steps:
1 CHOOSE THE MEDIA TO BE SHARED
2 CLICK THE «FORWA…
Forward
TELEGRAM.ME/NASHI…

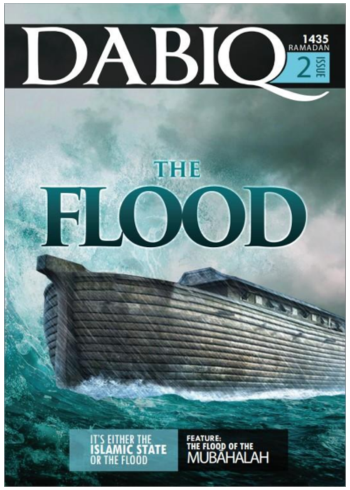
ISIS militant posts new execution vid…
https://www.youtube.com/wa…
16 Jun 2014 - Uploaded by CNN
An ISIS fighter posted videos depic…n of captured men and later an execution. Arwa Damon ...
2:57

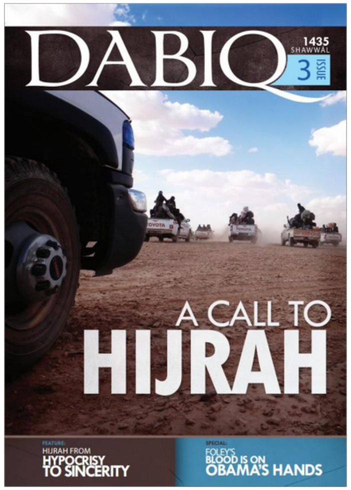
Home Notifications Messages Discover
Search Twitter
الدولة الإسلامية
@kjhgfdsasdf987
TWEETS 8,613
FOLLOWING 304
FOLLOWERS 4,447
FAVORITES 3,505
LISTS 7
Follow
Tweets Tweets & replies Photos & videos
Tweet to الدولة الإسلامية
4,306 Photos and videos

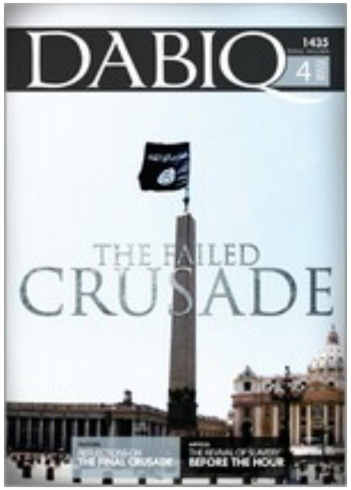
ICT for peace foundation

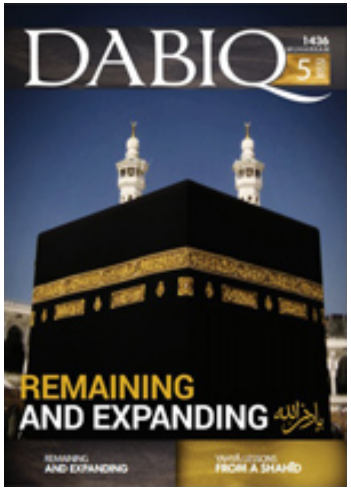
ISIS has published more than 10 issues of Dabiq totalling 250k words

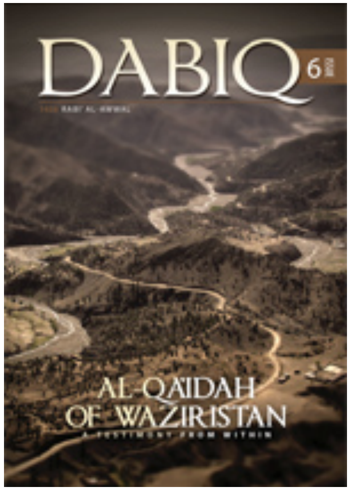


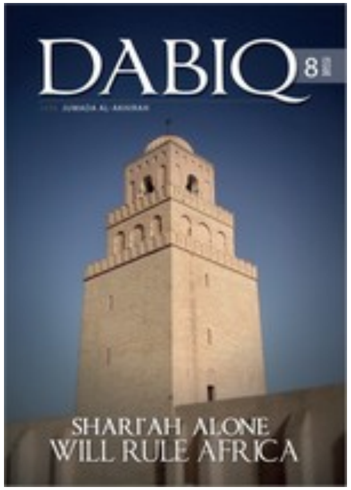

DABIQ
1435 RAMADAN
2 ISSUE
THE FLOOD
IT'S EITHER THE ISLAMIC STATE OR THE FLOOD
FEATURE: THE FLOOD OF THE MUBAHALAH

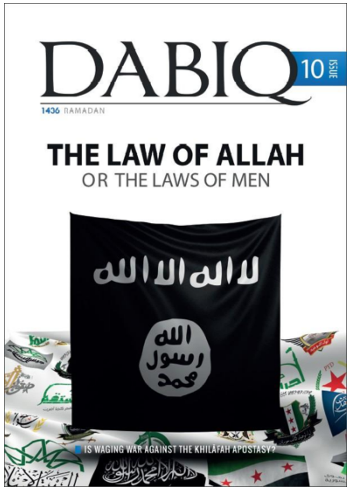

DABIQ
1435 SHAWWAL
3 ISSUE
A CALL TO HIJRAH
HIJRAH FROM HYPOCRISY TO SINCERITY
FOLEY'S BLOOD IS ON OBAMA'S HANDS


DABIQ
1435
4
THE FAILED CRUSADE
REFLECTIONS ON THE FINAL CRUSADE
THE REVIVAL OF SLAVERY BEFORE THE HOUR








DABIQ
10 ISSUE
1436 RAMADAN
THE LAW OF ALLAH OR THE LAWS OF MEN
لا اله الا الله
الله رسول محمد
IS WAGING WAR AGAINST THE KHILAFAH APOSTASY?

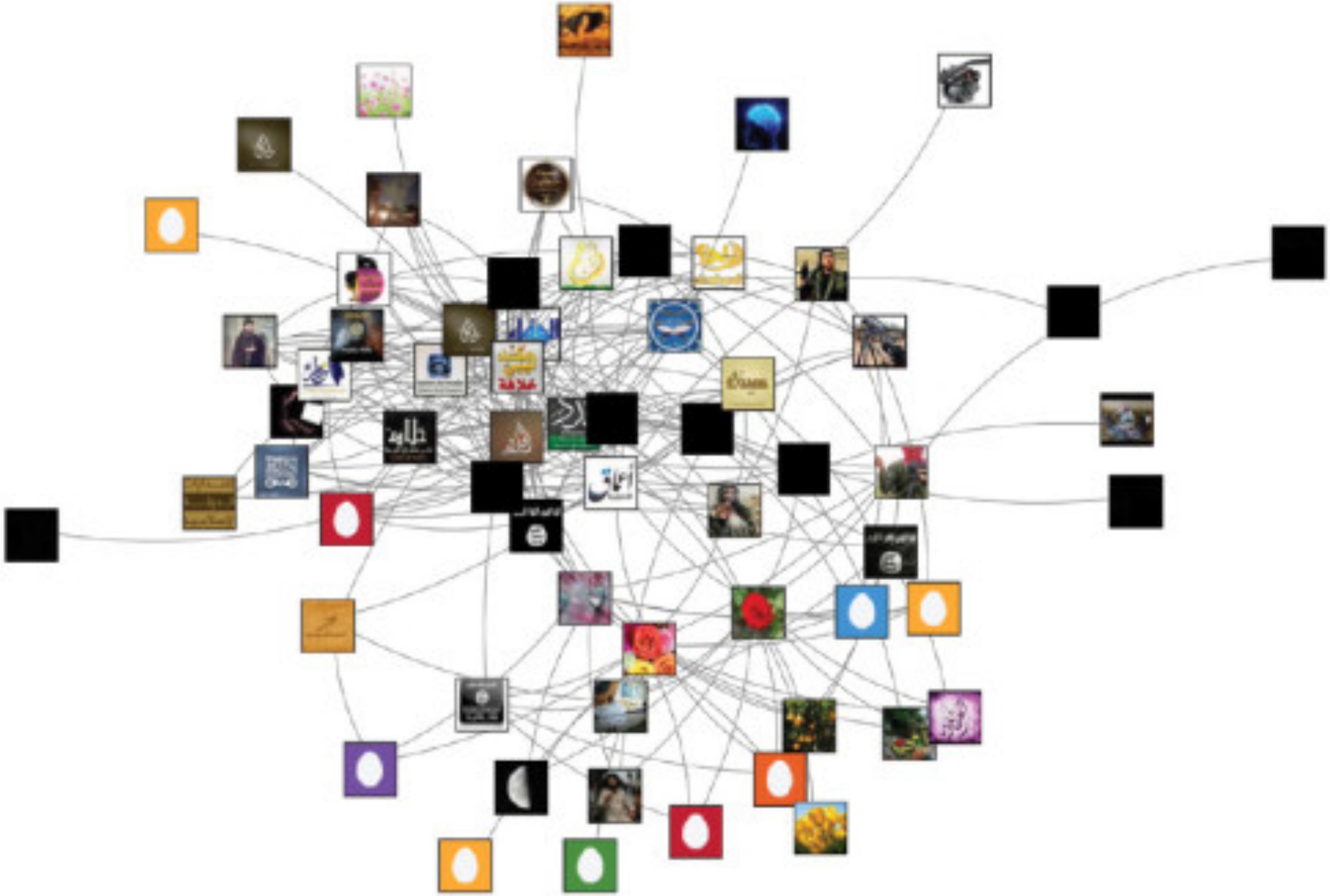
ICT for peace foundation

As “technological entrepreneurs” some terrorists have taken advantage of the internet and ICT to promote their propaganda and support operations

Operational Usage

- **Knowledge** transfer (**e.g. on how to make explosives, how to conduct attacks/ use of data location tools for planning purposes**)
- **Targeting** individuals (**e.g. identify and attack law enforcement through their social media profile – French case**)
- **Financing** operations
- **Command and Control (**through encrypted communications etc.)

What can be done: Social media network analysis or real-life social network analysis can support traditional policing and surveillance



ICT for peace foundation

A number of responses at national, regional and international levels relating to content management

National response

- **Requesting ICT companies to remove content based on Terms of Service (ToS)** and **violent content**
- Strategic communications operations e.g. **COUNTER** and **PREVENT** in the UK alongside its Research, Information, and Communications Unit (**RICU**)
- **US Madison-Valley-Wood Project** – US Government engagement with advertising, film (Hollywood) and tech sectors.
- **Internet Referral Units (IRU)** to pro-actively find material that violates the terms of service of social media companies
- Content filtering and requesting access to user data

International/ regional responses (some examples)

- **UN Security Council Presidential Statement** tasked Counter Terrorism Committee UN CTC) to develop plan for “comprehensive international framework” for countering the narratives of terrorist groups.
- Work of **UN Special Rapporteurs** on privacy, FoE and O
- **G7** recently launched its Plan on Countering Terrorism and Violent Extremism
- **European Commission’s** internet platform
- **EUROPOL** Internet Referral Unit (IRU) helping co-ordinate the response to terrorist-related content.
- **Council of Europe’s** report on content-related issues.

Industry responses

- **Proactive response**:
  - Twitter has suspended some 360,000 accounts since mid-2015.
  - Most of the large social media companies have large teams of analysts/ lawyers working on content requests.
  - Some also are working to develop algorithms to identify terrorists content.

- **Partly a reactive response** to government requests based on **Terms of Service (ToS)** and:
  - Information requests
  - Removal requests by private individuals
  - Copyright notices (DCMA)

- **Transparency reports** published by industry, incl. on what content taken down and on whose request

Key challenge = balancing existing norms such as freedom of expression, privacy and access to information with national/ int. security prerogatives

- **Important tensions** have emerged **between core rights and national security prerogatives**

i. **Freedom of expression and opinion, privacy, and the right to access information**

ii. **International Covenant on Civil and Political Rights (**ICCPR: "restrictions must be precise and public," and should be "more than merely useful, reasonable, or desirable"

- **Respect for core principles of transparency and accountability**

- **The challenge is how governments, international organisations, civil society organisation and technology companies can work better together (multi-stake holder approach)**

ICT for peace foundation

A growing number of emerging principles, norms and practices underpinning the tech. sector’s response to terrorist use of their products and services

- **Guiding Principles on Business and Human Rights**
- **European Commission’s ICT Sector Guide on Implementing the Principles**
- **Global Network Initiative’s (GNI) ”Principles on Freedom of Expression and Privacy”**
- **More recently the ICT4Peace-UN CTED initiative on the private sector engagement in responding to the terrorist use of ICT**

Our advisory group consists of a number of leading technology companies and a range of academic and civil society groups

UN CTED
Counter-Terrorism Committee
Executive Directorate

HOME

Microsoft

facebook

Google

新浪微博
weibo.com

EUROPOL

SecDev

KASPERSKY lab

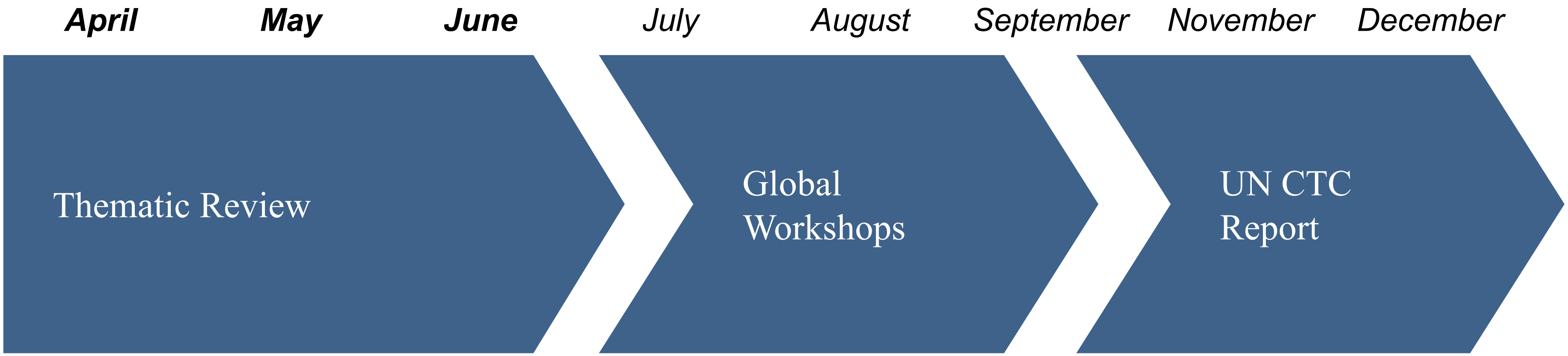
Institute of Strategic & International Studies (ISIS) Malaysia

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD

Global Network Initiative
Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies

In the first phase of the project, we will focus on delivering a Thematic Review and conducting 3 global workshops, which will feed into a report CTED will present to the UN CTC in November 2016


April ***May*** ***June*** *July* *August* *September* *November* *December*

Thematic Review

Global Workshops

UN CTC Report

ICT for peace foundation

Groups like IS and AQ might conduct cyber-enabled attacks against Critical Infrastructure (CI) or interrupt critical communications infrastructure.

- **The UN General Assembly's Group of Governmental Experts (GGE) 2015 noted:**

"The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility, which if left unaddressed may threaten international peace and security."

- Critical Infrastructure (CI): e.g. **global submarine fibre optic cable network or satellites, industrial control systems (ICS**), including **SCADA** (Supervisory Control and Data Acquisition) systems of critical infrastructure (**communications, transport, nuclear, electrical power grids, dam facilities and other forms of energy supplies, manufacturing facilities etc.).**
- **Challenges** include agreeing domestically and internationally on **what constitutes CI** *or* in relation to interpreting **the applicability of international law, for instance, to submarine cables in the high seas.**

ICT for peace foundation

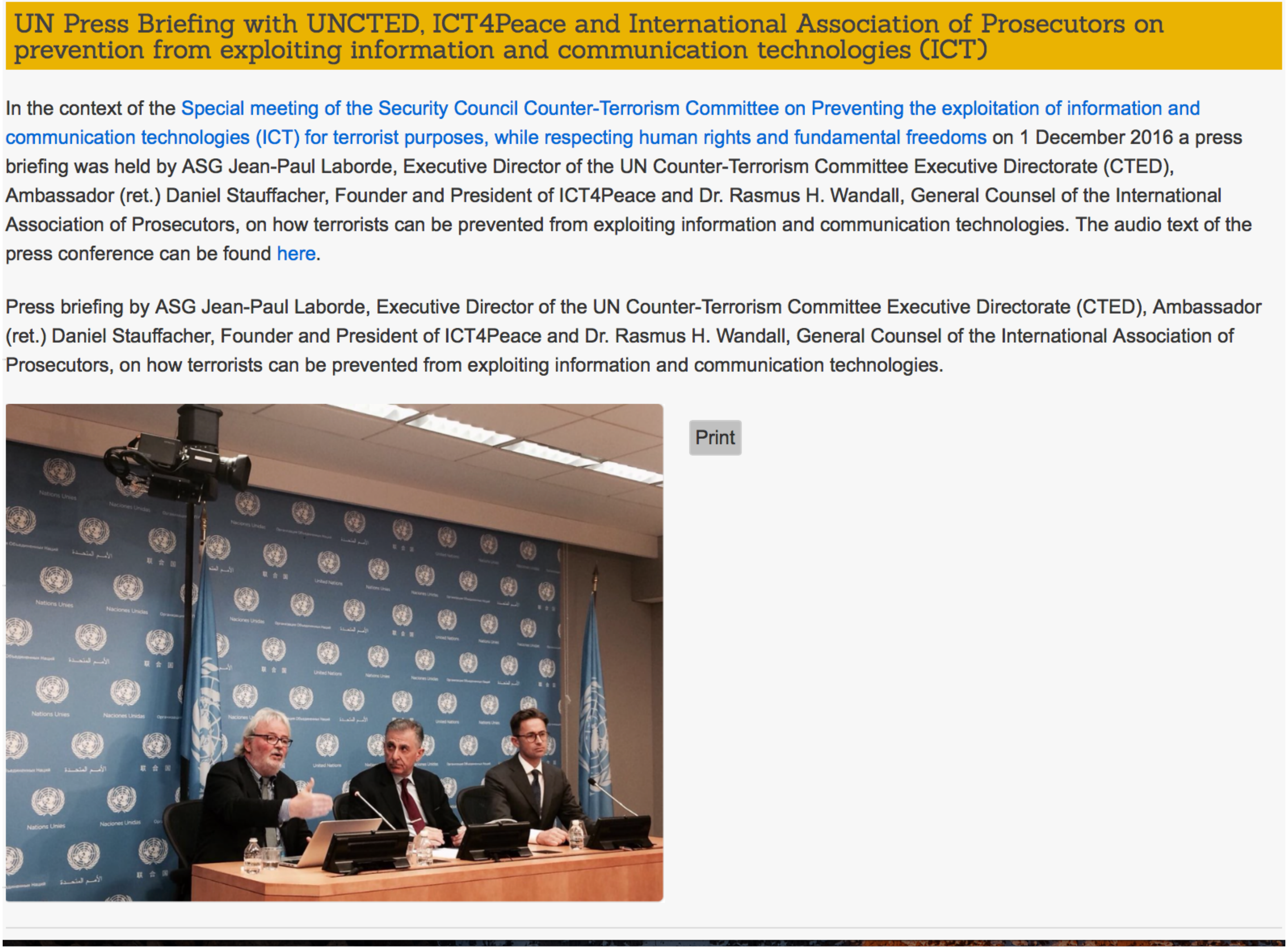
- .

Concern about growing reliance by governments on technology and technology-enabled solutions to resolve or manage highly complex issues such as radicalization and terrorism.

- Already in 2012 UN Counter Terrorism Implementation Task Force (UNCTTF) CTITF Working Group highlighted a basic but fundamental fact:

- *“**[t]echnology alone is no panacea for combating terrorism, including terrorist use of the Internet.** Technical approaches should be enshrined in appropriate legal frameworks, which – in turn – should be part of a comprehensive public policy response that support and clarify the role of technology in combating and countering terrorist activity on the Internet.”*

- **Undoubtedly, the continued tendency toward technological solutionism tends to ignore the very structural issues that led to terrorist-related activity in the first place** and relegates hard-earned principles such as participation, transparency and accountability in decision-making and national policy to a secondary role**.**
- .



UN Press Briefing with UNCTED, ICT4Peace and International Association of Prosecutors on prevention from exploiting information and communication technologies (ICT)

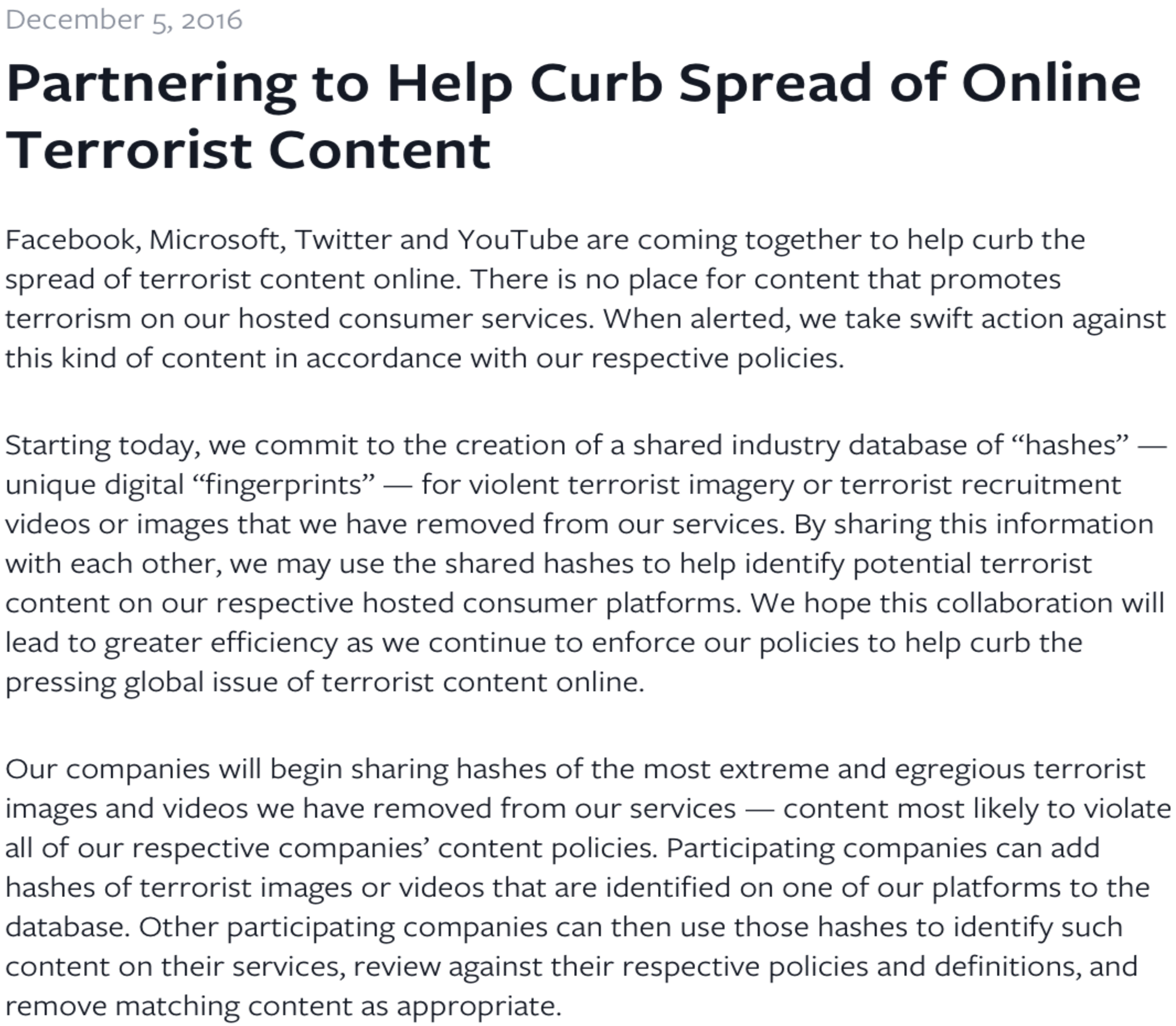
In the context of the Special meeting of the Security Council Counter-Terrorism Committee on Preventing the exploitation of information and communication technologies (ICT) for terrorist purposes, while respecting human rights and fundamental freedoms on 1 December 2016 a press briefing was held by ASG Jean-Paul Laborde, Executive Director of the UN Counter-Terrorism Committee Executive Directorate (CTED), Ambassador (ret.) Daniel Stauffacher, Founder and President of ICT4Peace and Dr. Rasmus H. Wandall, General Counsel of the International Association of Prosecutors, on how terrorists can be prevented from exploiting information and communication technologies. The audio text of the press conference can be found here.

Press briefing by ASG Jean-Paul Laborde, Executive Director of the UN Counter-Terrorism Committee Executive Directorate (CTED), Ambassador (ret.) Daniel Stauffacher, Founder and President of ICT4Peace and Dr. Rasmus H. Wandall, General Counsel of the International Association of Prosecutors, on how terrorists can be prevented from exploiting information and communication technologies.

Report on Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes

- The project findings point to the emergence of a voluntary policy framework guiding private and public action on responding to online terrorist content and activity.
- The voluntary framework recognizes the importance of enhancing public safety with actions that remain anchored in the rule of law, protecting and respecting human rights and core principles such as transparency, accountability, predictability and remedy.
- At the same time, there is a risk that this emerging policy framework may be undermined by some of the measures that are being taken in response to public security concerns posed by the growing incidence of terrorist use of the internet.
- These measures include restrictions, lawful or unlawful orders compelling companies to provide access to user data, and steps to increase greater state involvement in internet governance.
- Evidently, it is impossible to ignore the public security challenges relating to online terorrist activity and content. At the same time, both public and private actors should consider the longer-term prevention benefits of ensuring that the core principles I mentioned are respected.
- To this end we have put forward several recommendations. The first three relate to ongoing processes And include:
- - **Facilitating stronger and more sustainable dialogue** between civil society, technology companies, and governments
- - Helping **consolidate the emerging global policy normative framework on issues such as transparency and accountability**, as well as other practical concerns.
- - **Strengthening the links between OFFLINE Prevention and ONLINE Counter-Terrorism** and reinforce the role of human rights when developing and enforcing policy

Facebook, Microsoft, Twitter and Youtube and Terrorist Content



December 5, 2016

Partnering to Help Curb Spread of Online Terrorist Content

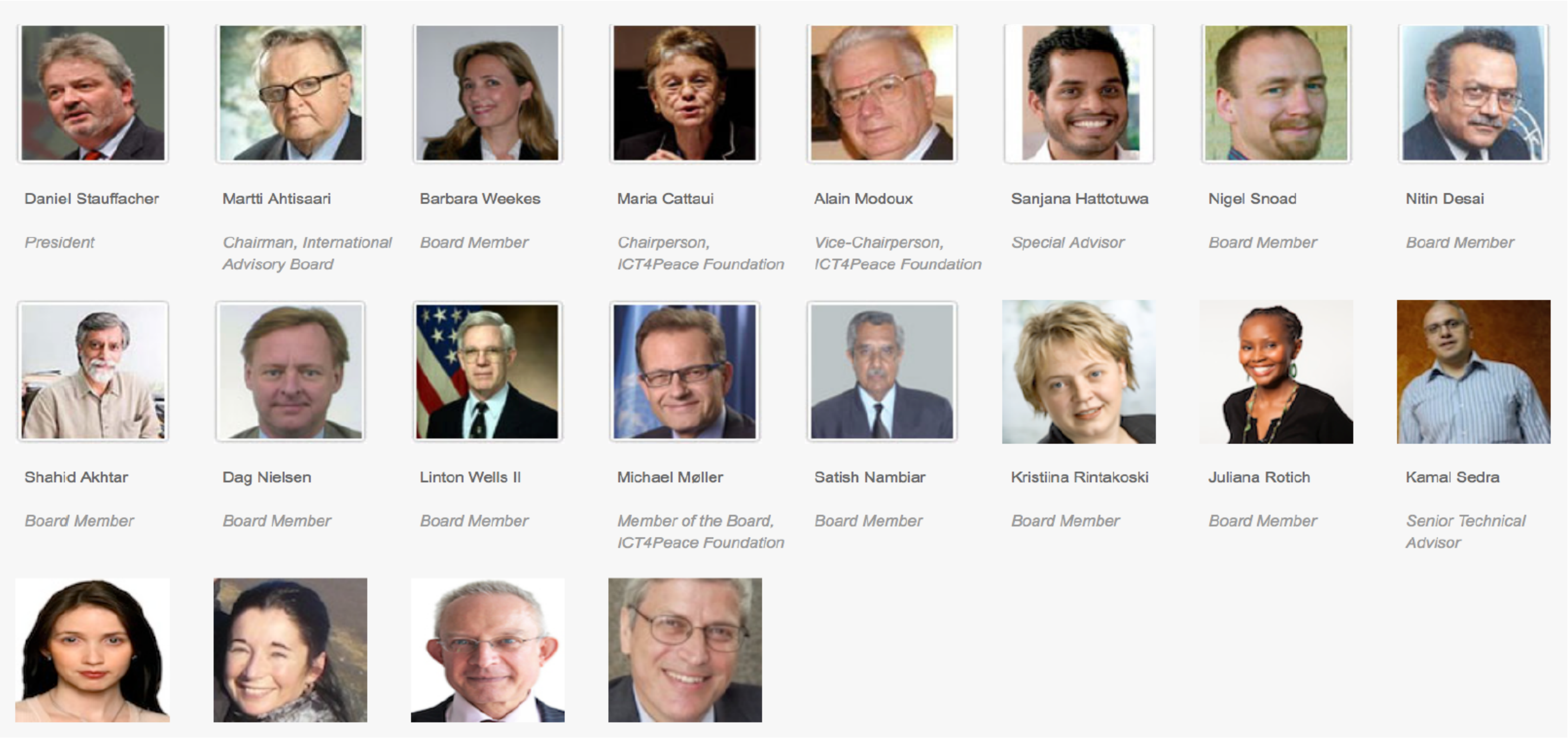
Facebook, Microsoft, Twitter and YouTube are coming together to help curb the spread of terrorist content online. There is no place for content that promotes terrorism on our hosted consumer services. When alerted, we take swift action against this kind of content in accordance with our respective policies.

Starting today, we commit to the creation of a shared industry database of “hashes” — unique digital “fingerprints” — for violent terrorist imagery or terrorist recruitment videos or images that we have removed from our services. By sharing this information with each other, we may use the shared hashes to help identify potential terrorist content on our respective hosted consumer platforms. We hope this collaboration will lead to greater efficiency as we continue to enforce our policies to help curb the pressing global issue of terrorist content online.

Our companies will begin sharing hashes of the most extreme and egregious terrorist images and videos we have removed from our services — content most likely to violate all of our respective companies’ content policies. Participating companies can add hashes of terrorist images or videos that are identified on one of our platforms to the database. Other participating companies can then use those hashes to identify such content on their services, review against their respective policies and definitions, and remove matching content as appropriate.

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

Vielen Dank – Merci Beaucoup

danielstauffacher@ict4peace.org