

ICTs for Peaceful Purposes and Peace in the Cyberspace

137th IPU Assembly

St. Petersburg, Russian Federation

14–18 October 2017

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



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**



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):

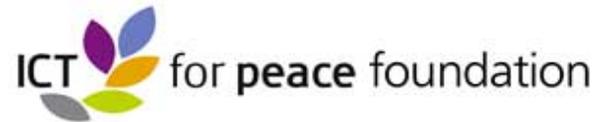
- *“36. We value the potential of ICTs to promote peace and to prevent conflict which, inter alia, negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian 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.

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
- **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.



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)**
- 3. Mandate by UN Security Council for Tech Against Terrorism (techagainstterrorism.org)**

Interim Report: Stocktaking of UN Crisis Information Management Capabilities

Sanjana Hattotuwa and Daniel Stauffacher

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

+ SUBMIT INCIDENT

Search Reports Here:

DOWNLOAD REPORTS (3531)

REPORTS RSS

HOME REPORTS SUBMIT INCIDENT GET ALERTS CONTACT US HOW TO HELP ABOUT

FILTERS → **REPORTS** NEWS PICTURES VIDEO TODO VIEWS → **CLUSTERS** ↓ CATEGORY FILTER

Terms of Use

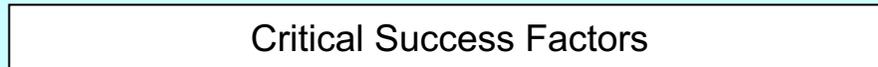
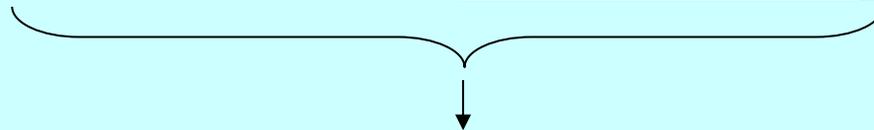
ALL CATEGORIES

1. URGENCES | EMERGENCY
2. URGENCES LOGISTIQUES | VITAL LINES
3. PUBLIC HEALTH
4. MENACES | SECURITY THREATS
5. INFRASTRUCTURE DAMAGE

Business Drivers



Technology Drivers



- Leadership
- Funding
- Evaluation
- Incrementalism



UN Secretary-General 2010 Crisis Information Strategy (A/65/491)

- ***Crisis information management strategy. The Crisis Information Management Strategy is based on the recognition that the United Nations, its Member States, constituent agencies and non-governmental organizations need to improve such information management capacity in the identification, prevention, mitigation, response and recovery of all types of crises, natural as well as man-made. The strategy will leverage and enhance this capacity and provide mechanisms to integrate and share information across the United Nations system.***
- The Office of Information and Communications Technology (CITO), together with the Office for the Coordination of Humanitarian Affairs (OCHA), the Department of Peacekeeping Operations and the Department of Field Support (DPKO and DFS), has worked closely with United Nations organizations such as the Office of the United Nations High Commissioner for Refugees (UNHCR), the United Nations Children's Fund (UNICEF), the United Nations Development Programme (UNDP) and WFP and other entities such as **the ICT for Peace Foundation** in developing and implementing this strategy. It is envisaged that membership will be expanded to include other United Nations organizations in the near future.

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

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-



Implement UN Crisis Information Management With UN CIM Advisory Group CiMAG)

UN Crisis Information Management Advisory Group (CiMAG) retreat looks at Ebola response



ICT4Peace was again invited by **ASG UN Chief Information Technology Officer Ms. Atefeh Riazi** to organise again the UN Crisis Information Management Retreat (CIMAG) 2015. The themes of this year's retreat were as follows:

- An introspection of the UNMEER / UN Ebola response, interrogating in particular the adoption of Crisis Information Management (CiMS) principles to strengthen collaboration and coordination in the response efforts
- A retrospection of CiM efforts of the UN since Haiti 5 years ago, ending with UNMEER, to understand what's changed and what remain key

challenges.

- Moving forward, develop concrete recommendations for the UN top Management on how data and technology can be better leveraged within the UN system and beyond to manage humanitarian crisis such as Ebola.

Approximately 30 Information Management Specialists from the UN Secretariat, UN Organisations responsible for Peacekeeping, Peacebuilding and Humanitarian Operations participated on 8 and 9 June in Manhattan New York Meeting (UN OICT, OCHA, WHO, DPKO/DFS, UNDP, UNICEF, World Bank, UNOSAT, UNMEER, UNHCR, UN OCC, UN DPA, UN DPI, UN Global Pulse).

Further Applications of ICTs: Prevention of mass atrocity crimes, ICTs for election monitoring, Constitution building, Combating hate speech, “fake news” etc.



SEARCH



UPDATES



PUBLICATIONS



FEATURED ARTICLES



KEY REPORTS



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

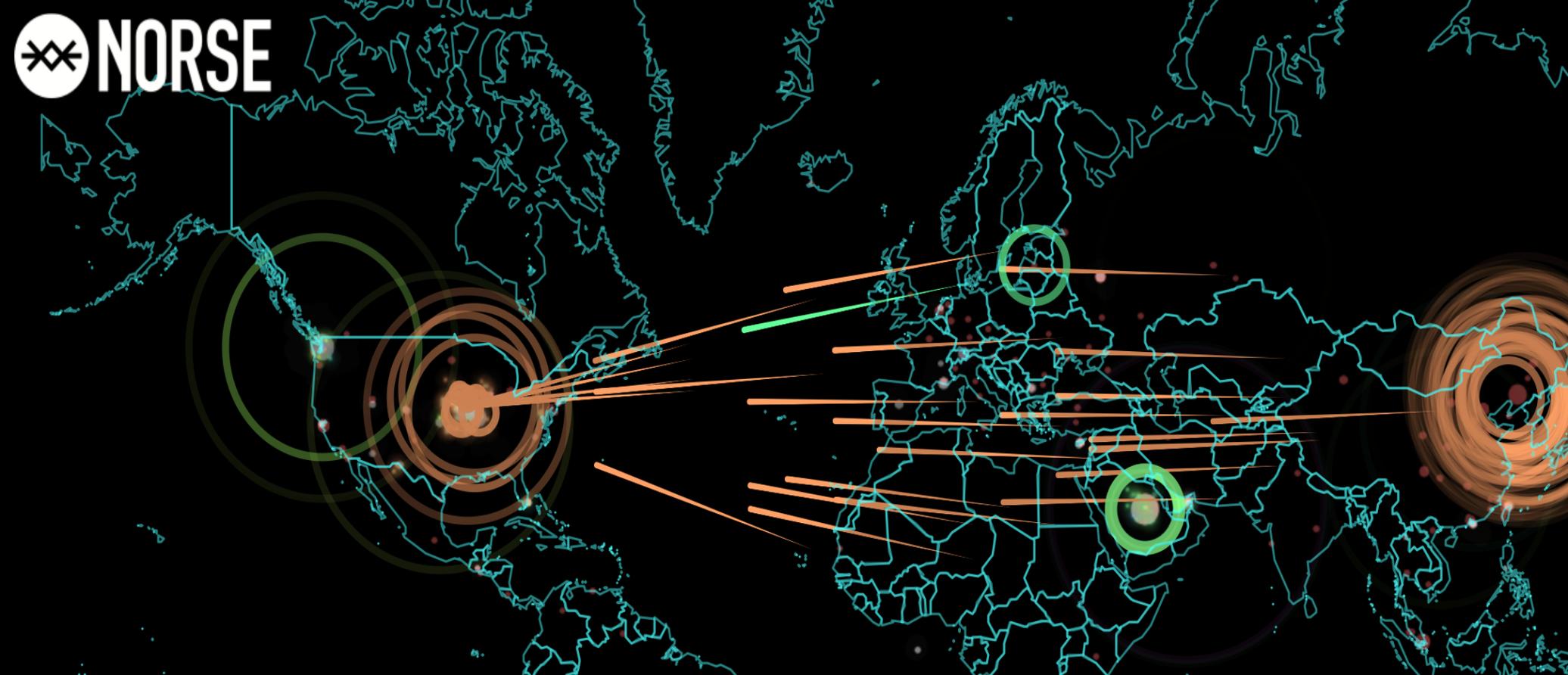
Lessons for Myanmar?

Sanjana Hattotuwa

TED Fellow alumn, ICT4Peace Foundation

At the invitation of the Myanmar Information Management Unit (MIMU), Sanjana Hattotuwa conducted a presentation on the dangers of social media and in response to the strategic deployment of services and speech as well as election monitoring and education.

The discussion lasted for a half hour.



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 Emirates
20	Russia
15	Taiwan
15	Bulgaria
11	Hong Kong
11	Saudi Arabia

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
09:00:24.66			Riyadh, SA	Riyadh, SA	unknown	137

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 undermines confidence and trust between states, and between states and citizens.**

The Cyber Security Challenge: What Can be Done at the National level ? Some Examples

- **Building National Cybersecurity Strategies for Governments, Business and Civil Society**
- **Passing national Cybersecurity Legislation, including cybercrime, data protection etc.**
- **Building National Computer Emergency Response Teams (CERT)**
- **Cybersecurity Capacity Building Programmes**
- **Cybersecurity Public Private Partnerships**

The Cyber Security Challenge: What Can be Done at the International level ?

- 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/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

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.



**Organization for Security and Co-operation in Europe
Permanent Council**

PC.DEC/1202
10 March 2016

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;

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).**

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 specific cyber security-related confidence building measures (CBMs) for the Asia-Pacific region.

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.

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.**

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.

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 Commitment and was completed the UN General Assembly in December 2015.**
- **Sustainable Development Goals (SDGs) approved in December 2015**

Critique: UN Millenium Declaration 2000

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)**
- **ORGANISATION OF AMERICAN STATES (OAS)**
- **AFRICAN UNION**
- **NORTH ATLANTIC TREATY ORGANISATION (NATO)**
- **EUROPEAN UNION**

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.**

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

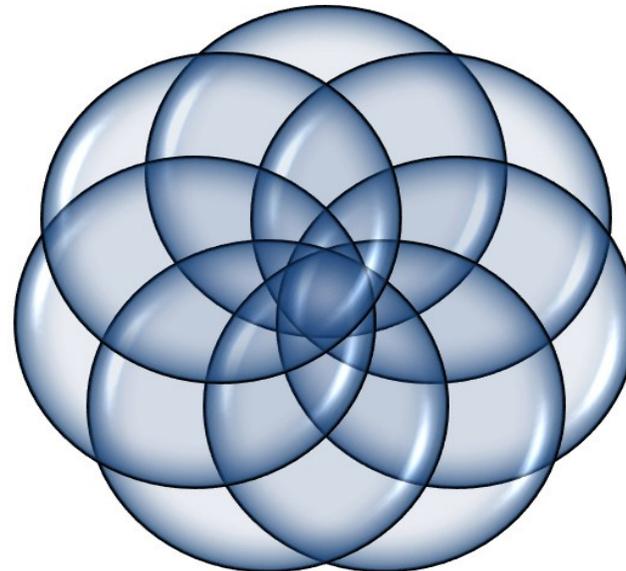
- UK
- US
- EU
- Germany

GERMANY

- US
- India
- China

INDIA

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



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



¿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



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



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

CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY

GENEVA 2013
ICT4PEACE FOUNDATION

ICT4Peace and OAS workshop on International Security and Diplomacy in Cyberspace with 50 Diplomats and Technical Staff from 26 Countries (Bogota, Colombia, November 2014)



ICT4Peace Cybersecurity policy and diplomacy capacity building with African Union



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



Department 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





Singapore – ICT4Peace Foundation Joint Programme
“Capacity Building for International Cyber Security Negotiations”
19 to 20 October 2015
Furama City Centre, Singapore

ICT4Peace Cybersecurity policy and diplomacy capacity building program on Norms, CBMs with Governments and Regional Organisations.



Ministry of Foreign Affairs of the Kingdom of Thailand
กระทรวงการต่างประเทศ

The Ministry of Foreign Affairs, the National Security Council and Ministry of Digital Economy of the Kingdom of Thailand had invited ICT4Peace to contribute to the Regional Workshop on Cybersecurity: Norms in Cyberspace for ASEAN Countries on 19 and 20 December 2016 in Bangkok.

The objective of the two day workshop was to bring brought discussions about norms in cyberspace and both editions of the Tallinn Manual on the International Law Applicable to Cyber Warfare to the regional context, and to explore possible implications on the region and how ASEAN Member States can contribute to the efforts to develop internationally accepted norms in Cyberspace.

The speakers and lecturers at the workshop included:

- Mr. Vichit Chitvimarn, Ambassador attached to the Ministry of Foreign Affairs of the Kingdom of Thailand
- Mr. Vera Urairat, Deputy Secretary-General of the National Security Council of the Kingdom of Thailand
- Dr. Chaichana Mitran, Deputy Executive Director of the Electronic Transactions Development Agency (ETDA) under the Ministry of Digital Economy and Society of the Kingdom of Thailand
- Dr. Kriangsak Kittichaisaree (UN International Law Commission)
- Ms. Danielle Yeow (Attorney-General's Chambers of Singapore)
- Dr. Eneken Tikk-Ringas (ICT4Peace Foundation; ISGA, Leiden University)
- Dr. Mika Kerttunen (ICT4Peace Foundation)
- Dr. Daniel Stauffacher (President ICT4Peace Foundation)

This workshop can be considered first of its kind, where Governments informally reflected at the regional level (ASEAN) on how to contribute to the debate at the global level to develop voluntary norms, rules and principles of responsible State behavior.

ASEAN CYBER NORMS WORKSHOP 8 - 9 MAY 2017 SINGAPORE



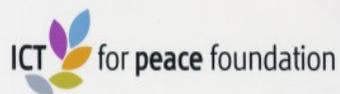
Organised by:



As an initiative under:



In collaboration with:



The Cyber Security Agency (CSA) of Singapore, in collaboration with ICT4Peace Foundation, held the inaugural ASEAN Cyber Norms Workshop in Singapore from 8 to 9 May 2017 under the auspices of Singapore's ASEAN Cyber Capacity Programme.

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

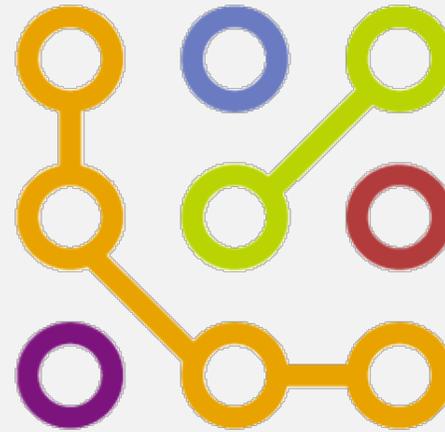
In addition to forty senior-level participants from ASEAN Governments, thirteen Senior Diplomats from and Experts from Australia, China, Egypt, Germany, Indonesia, Japan, Malaysia,

Netherlands, United States, Finland and Estonia participated. These countries are also members of the ongoing UN GGE. ICT4Peace, which was invited by Singapore to collaborate in the organisation of this workshop, was represented by Dr. Eneken Tikk, Dr. Mika Kerttunen and Dr. Daniel Stauffacher.

Second ICT4Peace Cybersecurity policy and diplomacy Workshop for CLMV Countries in Hanoi (12 and 13 October 2017)



tech against terrorism



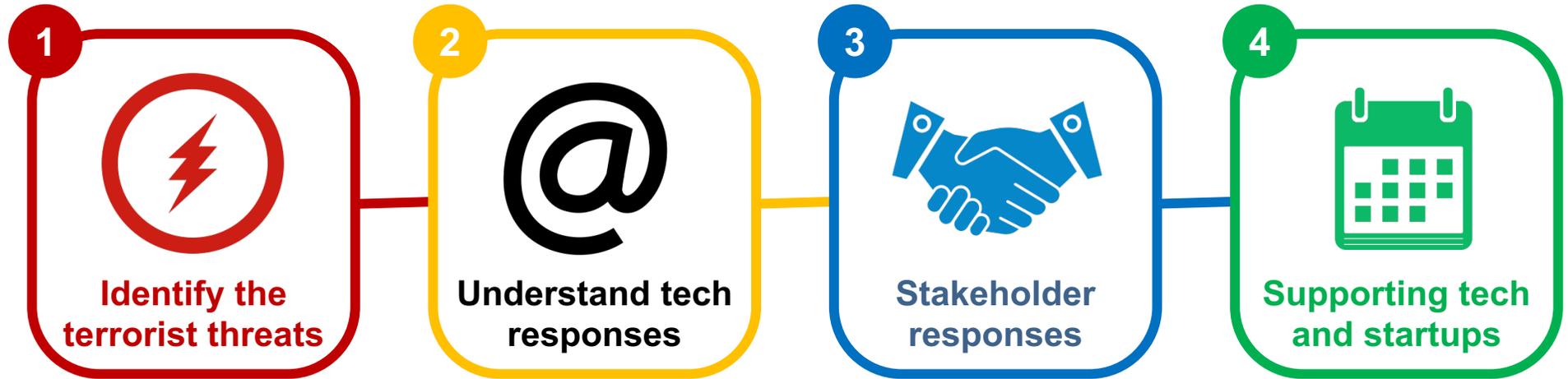
Connecting industry, government, and civil society to prevent the terrorist use of the internet whilst respecting human rights

techagainstterrorism.org @techvsterrorism

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



In 2016 we laid the foundations for the Tech Against Terrorism Project through a series of global workshops



- 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?

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



In the second project phase 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)

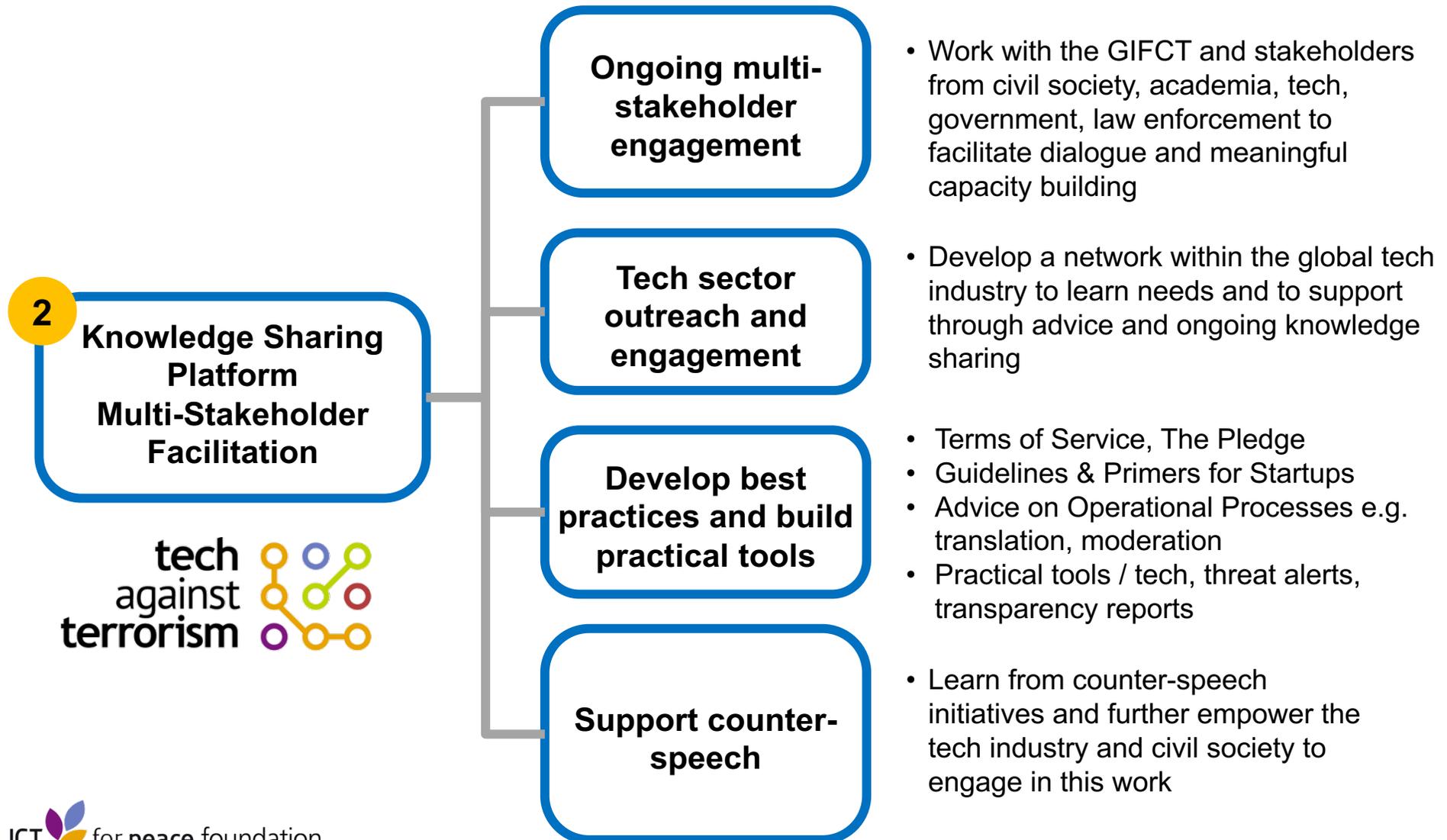


Communications and messaging

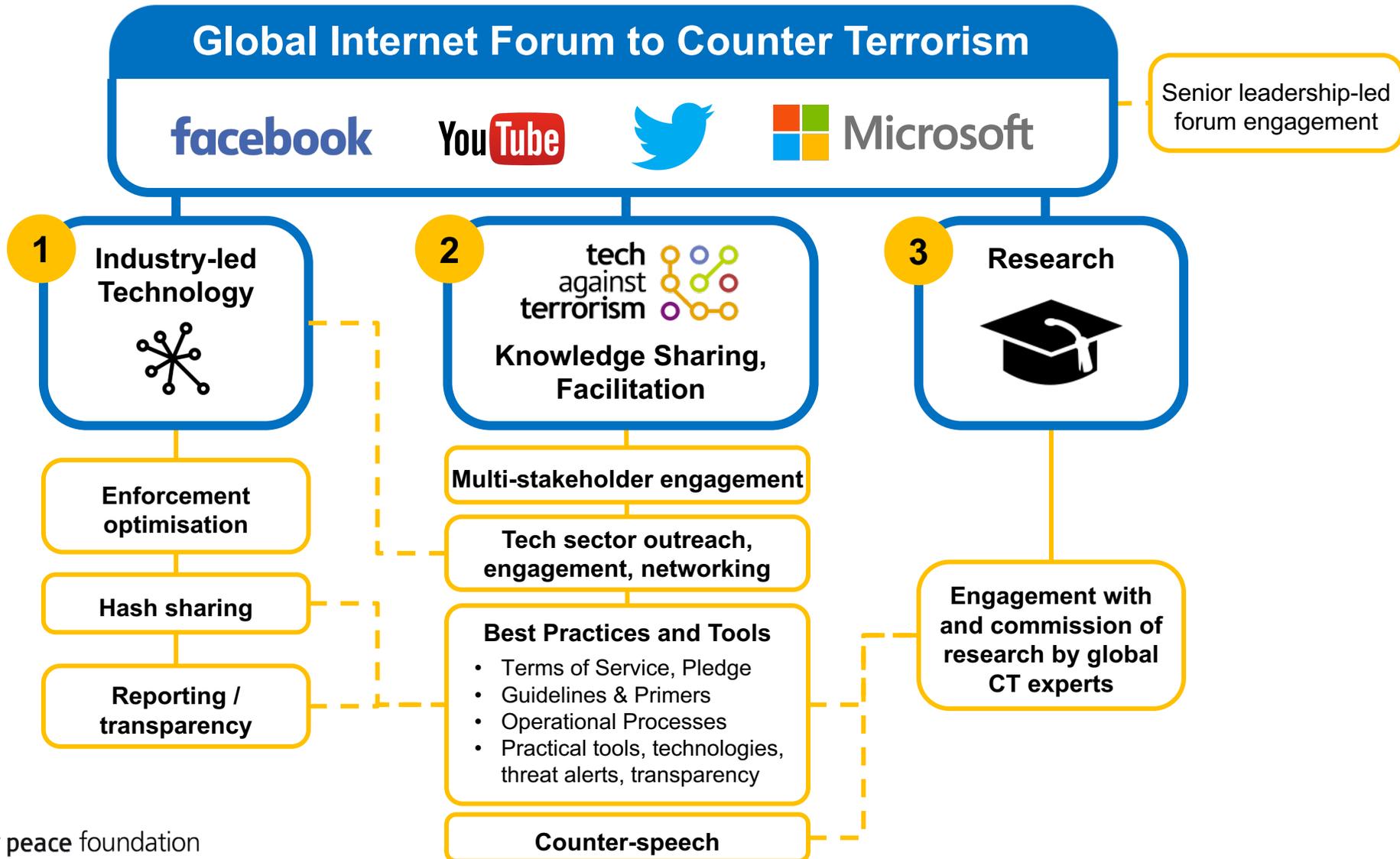


Financial funding and transfers

We developing an online Knowledge Sharing Platform (KPS) and facilitating ongoing engagement with the wider tech industry



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



Merci Beaucoup

danielstauffacher@ict4peace.org