

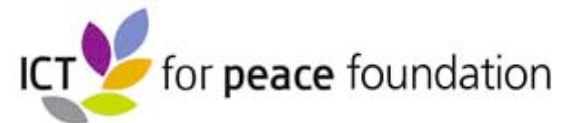
“Meeting the Cyber Security Challenge - 19”

Geneva Center for Security Policy

2. October 2019

Daniel Stauffacher

ICT4Peace Foundation



highlights

FR | SP | DE



The Second Phase of WSIS: Tunis 2005

The second phase of the WSIS was held in Tunis on November 16-18 2005. The outcome documents were the Tunis Commitment <http://www.itu.int/wsis/docs2/tunis/off/7.html> and Tunis Agenda for the Information Society <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

Swiss statements in Tunis 2005



Swiss President Samuel Schmid's speech during the WSIS Opening Ceremony November 16 2005.

<http://www.bundespraesident.admin.ch/internet/president/en/home/redint/reden2005/051116b.html>

- → [Archived Speech available here \(English\)](#)
- → [Archived Speech available here \(French\)](#)



Two statements from Federal Counsellor Moritz Leuenberger, head of the Federal Department of Environment, Transport, Energy and Communications, during the plenary session <http://www.uvek.admin.ch/dokumentation/reden/chef/20051117/02407/index.html?lang=fr> of November 17 2005 and at the occasion of the Summit closing ceremony

<http://www.uvek.admin.ch/dokumentation/reden/chef/20051118/02408/index.html?lang=fr>

→ [Archived Speech available here \(French\)](#)

NEWS IN SECOND PHASE OF THE WSIS

- Information and Communications Technology for Peace: The role of ICT in preventing, responding to and

contact

sitemap

WSIS executive secretariat

civil society platform

new info

3 April 2007

Cluster of WSIS-related events 2007: Online registration is now open

2 April 2007

Action Line C7 e-agriculture: FAO press release - "e-Agriculture should focus on Information over Technology"



Photo © ITU/Andre Longchamp

President Pascal Couchepin's Opening Speech at the World



WSIS+15 FORUM 2020

30 March - 3 April
Geneva, Switzerland

Fostering digital transformation and global partnerships:
WSIS Action Lines for achieving SDGs

High-Level

Contribute &
Participate

Win & Share

Sponsor

Innovate

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



The UN World Summit on the Information Society (WSIS) in Tunis 2005

- Paragraph 36 of the World Summit on the Information Society (WSIS) Tunis Declaration (2005):

- *“36. We value the potential of ICTs to promote peace and to prevent conflict which, inter alia, negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction.”* between peoples, communities and stakeholders involved in crisis management, humanitarian aid and peacebuilding.

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organisations, companies and non-state actors.

OUR MISSION



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; UN Crisis Information Management Strategy
2. Since 2007 Promotion of Peace and Security in the Cyberspace (to maintain an open, secure, stable, accessible and peaceful ICT environment (International, Norms, CBMs, Capacity Building = OEWG, UN GGE, OSCE, ASEAN, ARF, OAS, AU) Law
3. 2016 Mandate by UN Security Council for regarding Prevention of Use of ICTs for Terrorist Purposes (also called Tech Against Terrorism).
4. Artificial Intelligence (AI), Lethal Autonomous Weapons Systems (LAWS) and Peace Time Threats in Cooperation with Zurich Hub for Technology (ZHET) +ETH + Industry
5. AI, Fake News and Democracy in cooperation with ZHET

Interim Report: Stocktaking of UN Crisis Information Management Capabilities

Sanjana Hattotuwa and Daniel Stauffacher



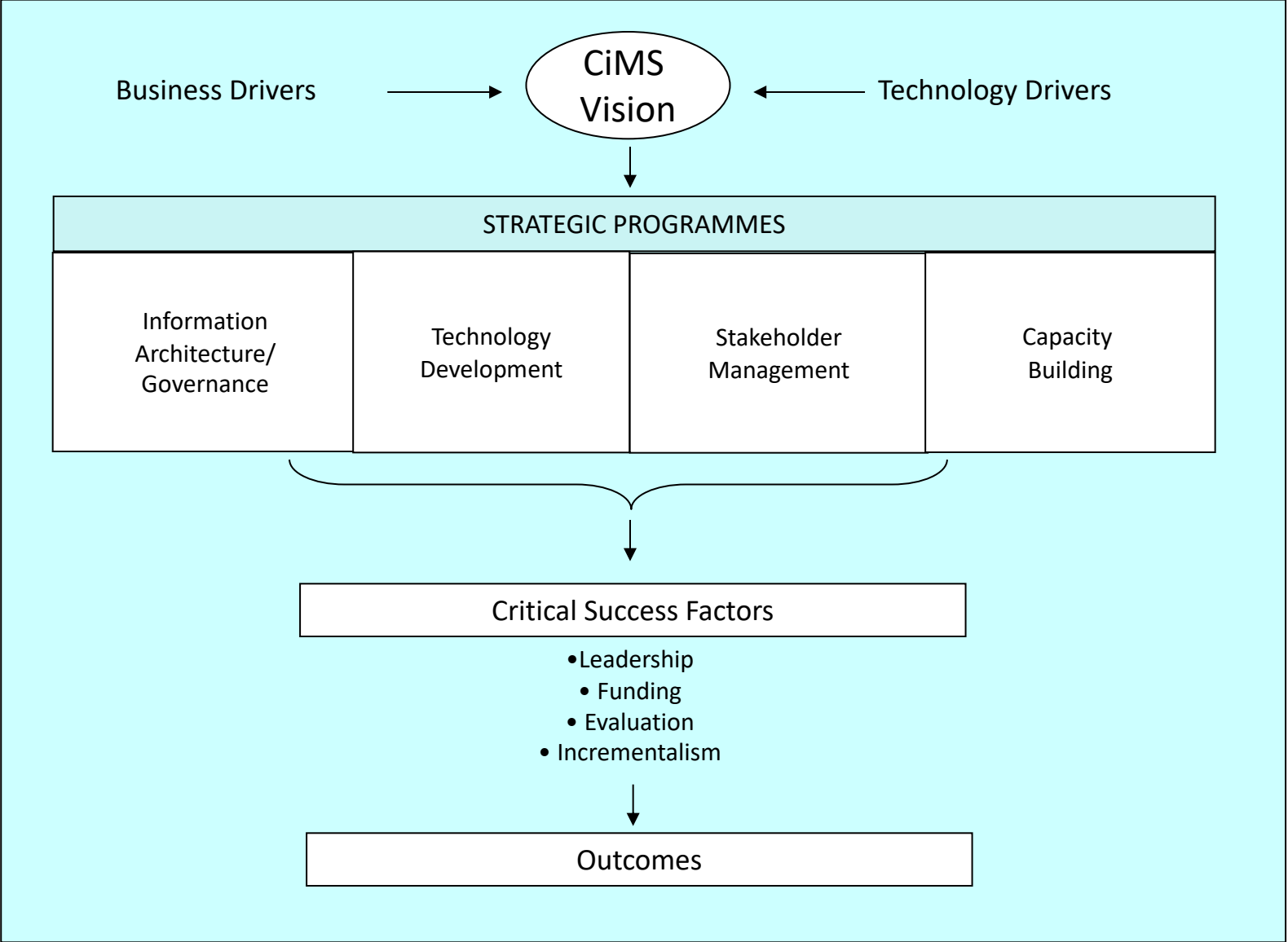
UN Secretary-General 2010 Crisis Information Strategy (A/65/491)



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.



New Tools: 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**

Search Reports Here:

[DOWNLOAD REPORTS \(3531\)](#)

[REPORTS RSS](#)

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](#)

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

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

ALL CATEGORIES

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

Information break-down in crisis situation



Improving
Crisis
Information
Management
in the Field:
MONUSCO



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

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

Navigate a new paradigm: Crisis Information Management Training Course

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



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-



The future of (UN) peacekeeping

- In June 2014, UN Under-Secretaries-General Hervé Ladsous (DPKO) and Ameerah Haq (DFS) announced the appointment of a [five-member Expert Panel](#), lead by ASG Jane Holl Lute, to advise them on how best to use new technologies and innovations to benefit United Nations peacekeeping to be [“a force for peace, a force for change, and a force for the future.”](#) (See also [here](#)).
- Along with other partner organisations, ICT4Peace’s Daniel Stauffacher was invited to discuss with the UN Expert Panel inter alia the following questions:
 - What available technologies have the potential for improving the conduct of peace operations?
 - (How) are they employed by the United Nations and other organizations? What lessons have been learned?
 - What are the challenges evolving around the use of these technologies? How can they be addressed properly?
- <https://ict4peace.org/activities/contributions-to-un-expert-panel-on-technology-and-innovation-in-peace-operations/>

Social media and peacekeeping

- Looking at four key opportunities, Sanjana noted the ability to and importance of engaging the last mile (i.e. local communities, directly) over social media, how a better understanding of complexity could help stronger strategic interventions, how social media was already inextricably entwined in the governance frameworks of many countries and contexts, and finally, how it could be used to reach out to a new, younger demographic in support of mission, mandate and UN writ large.
- <https://ict4peace.org/activities/crisis-information-management-capacity-building/implications-of-the-reforms-on-peace-operations-presentation-to-un-dsrsg-group/>



Implications of Social Media for Reformed Peace Operations: ICT4Peace Presentation to UN Leadership Group

AI disinformation and misinformation, Activities, Policy Research ICT, Capacity Building ICT, AI, LAWS and Peace Time Threats, UN Crisis Information Management Strategy (CIMS), Crisis Information Management Capacity Building, Strategic Input into UN peacekeeping, peacebuilding and humanitarian operations, ICTs and Human Rights Protection, New media for crisis management and peacebuilding



© 12. FEBRUARY 2019

Sanjana Hattotuwa, Special Advisor at the ICT4Peace Foundation, was invited by the [Centre for International Peace Operations \(ZIF\)](#) to give a presentation on the impact of social media around political dynamics in mission contexts to a meeting of [Deputy Special Representatives of the Secretary-General \(DSRSGs\)](#) held in Berlin, 11-12 February 2019.

The agenda of the two-day meeting was anchored to a number of enduring, pressing or prescient challenges around peacekeeping and peacebuilding. These included the role of women and gender, early warning, intervention, the role and relevance of DSRSGs and mandates.

Sanjana's presentation, embedded below, can be downloaded as a PDF or PPT [here](#).

Technology and conflict mediation

- How will streams of narratives in multiple forms of storytelling and media impact the framing of peace mediation?
- What if the next billion coming online and using social media have a very different understanding of the normative values of peace mediation, based on liberal democracy and judeo-Christian values? Will the negotiation of difference around a mediation process be its own driver of violence?
- How can peace mediators and a mediation process sift the noise generated by social media, from what is actionable intelligence that can help shape the discussions, and the contours of the mediation process?
- <https://ict4peace.org/activities/policy-research/policy-research-ict/the-janus-effect-social-media-in-peace-mediation/>

The Janus Effect: Social Media in Peace Mediation

AI disinformation and misinformation, Policy Research ICT, Advisory ICT, AI, LAWS and Peace Time Threats, Reports, UN Crisis Information Management Strategy (CIMS), Strategic Input into UN peacekeeping, peacebuilding and humanitarian operations, ICTs and Human Rights Protection, New media for crisis management and peacebuilding, Big data

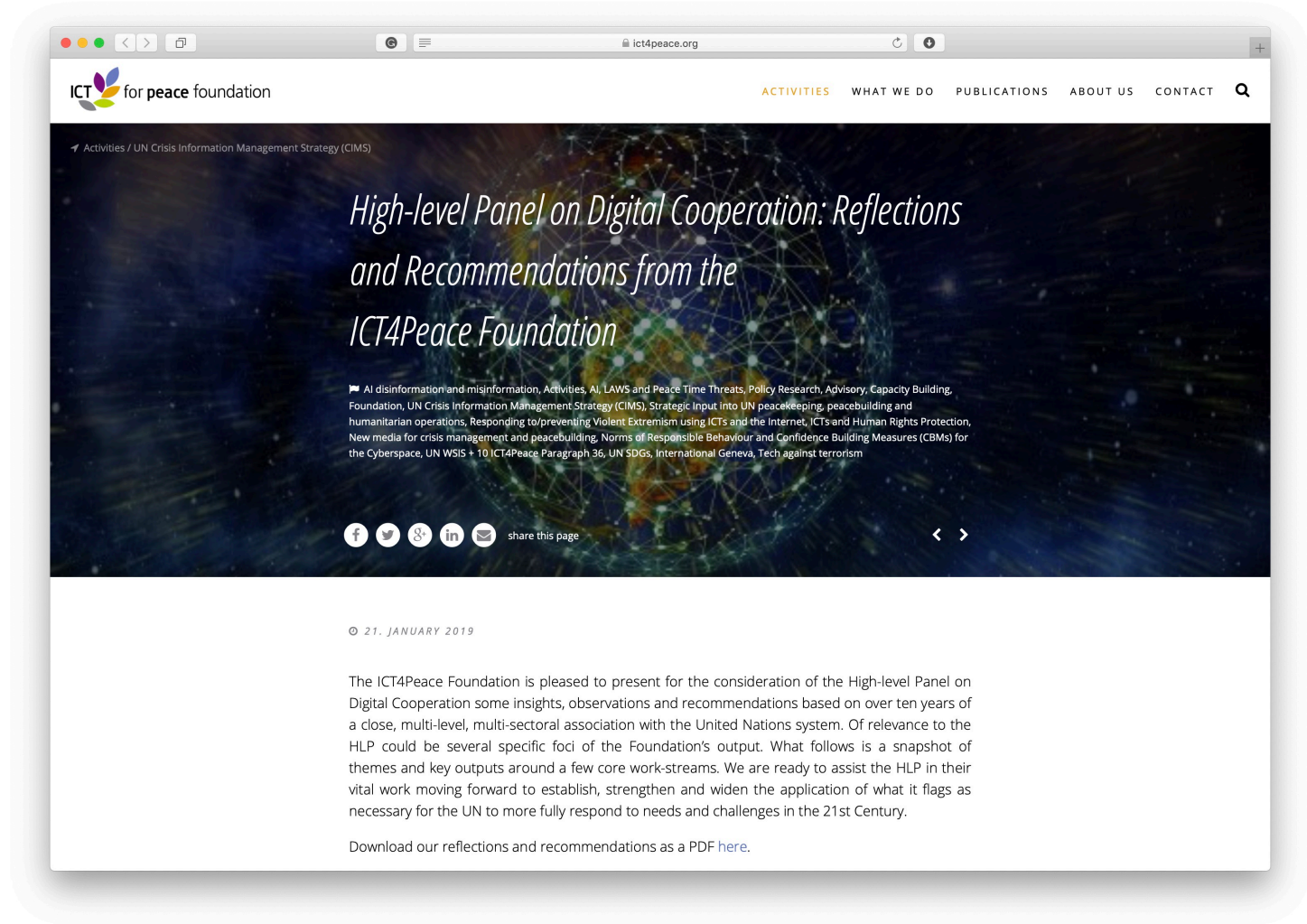
share this page

© 10. JULY 2018

The Janus Effect: Social Media in Peace Mediation

Sanjana Hattotuwa
ICT4Peace Foundation

Input into
the UN's HLP
on Digital
Cooperation




HIGH-LEVEL PANEL ON DIGITAL COOPERATION

HIGH-LEVEL PANEL ON DIGITAL COOPERATION

REFLECTIONS AND RECOMMENDATIONS FROM
THE ICT4PEACE FOUNDATION

Sanjana Hattotuwa, Barbara Weekes, Regina Surber & Daniel Stauffacher

 ICT for peace foundation

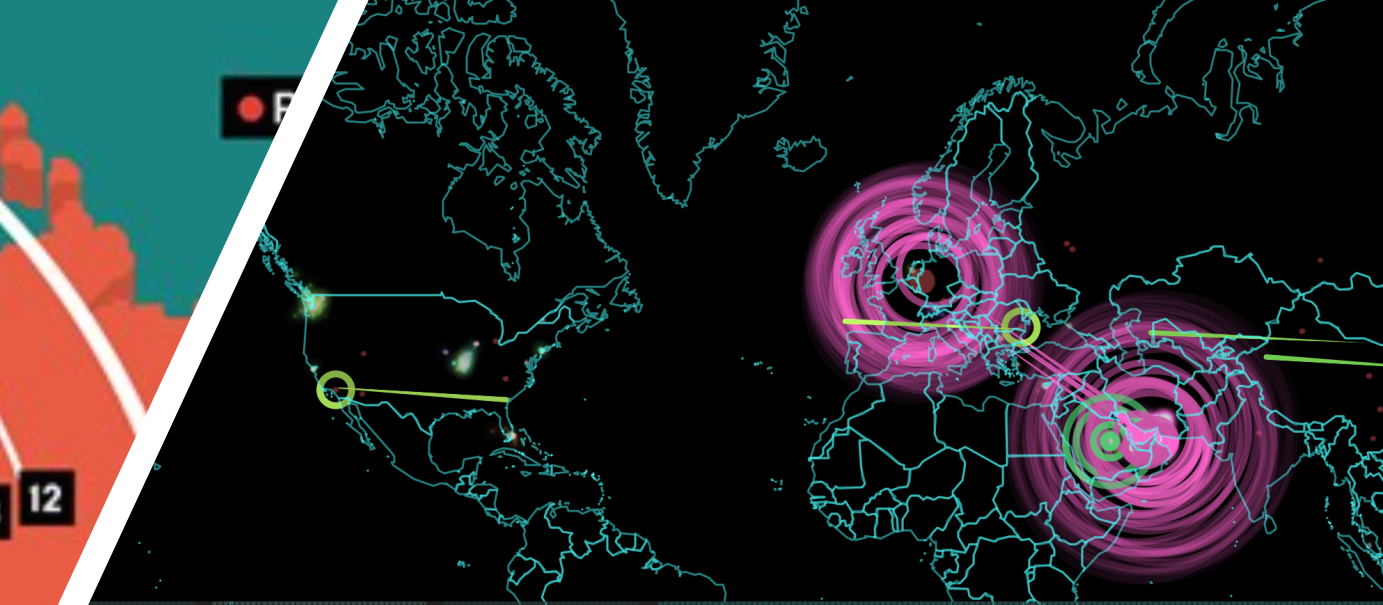
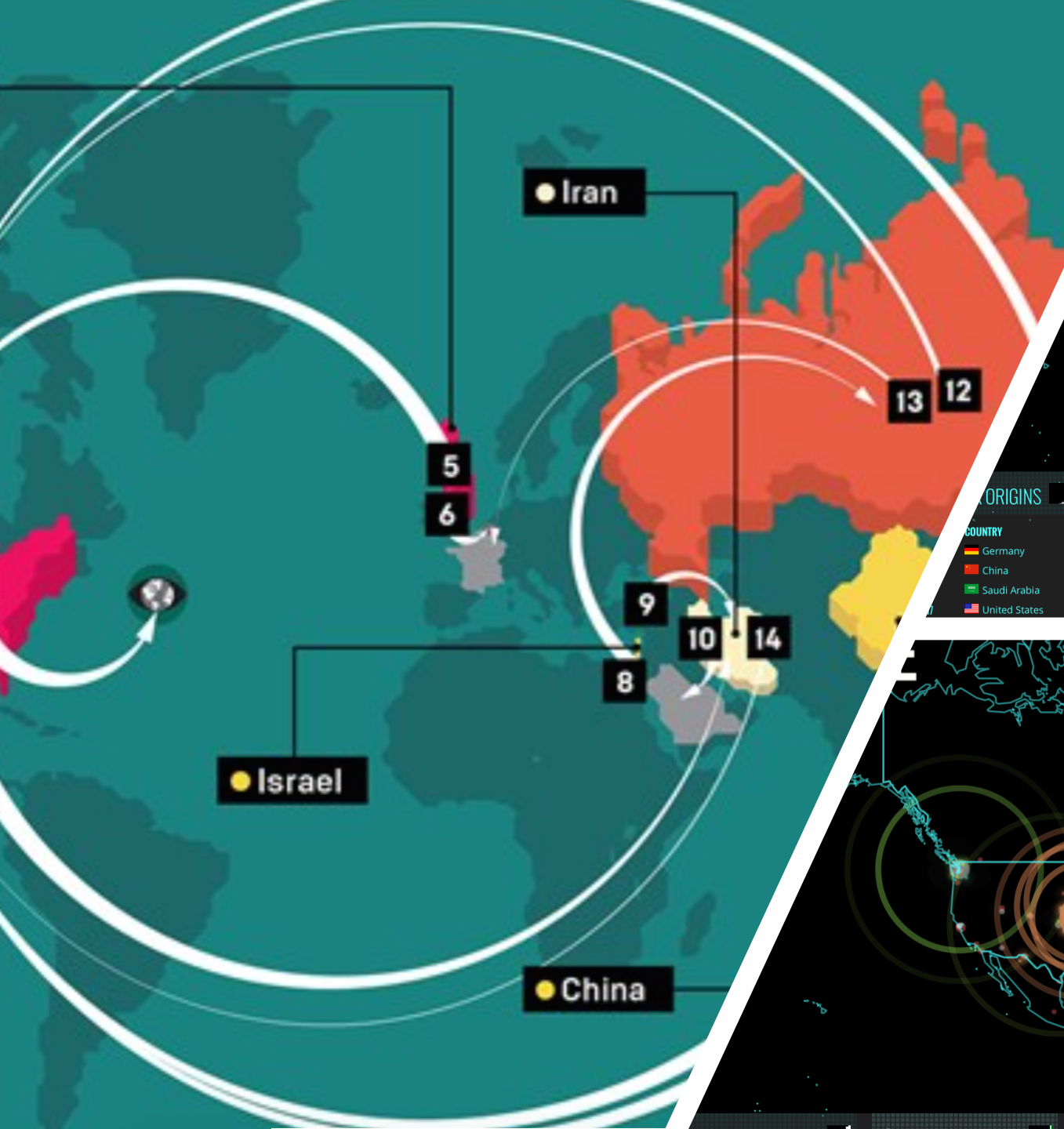
 ICT for peace foundation

HIGH-LEVEL PANEL ON DIGITAL COOPERATION

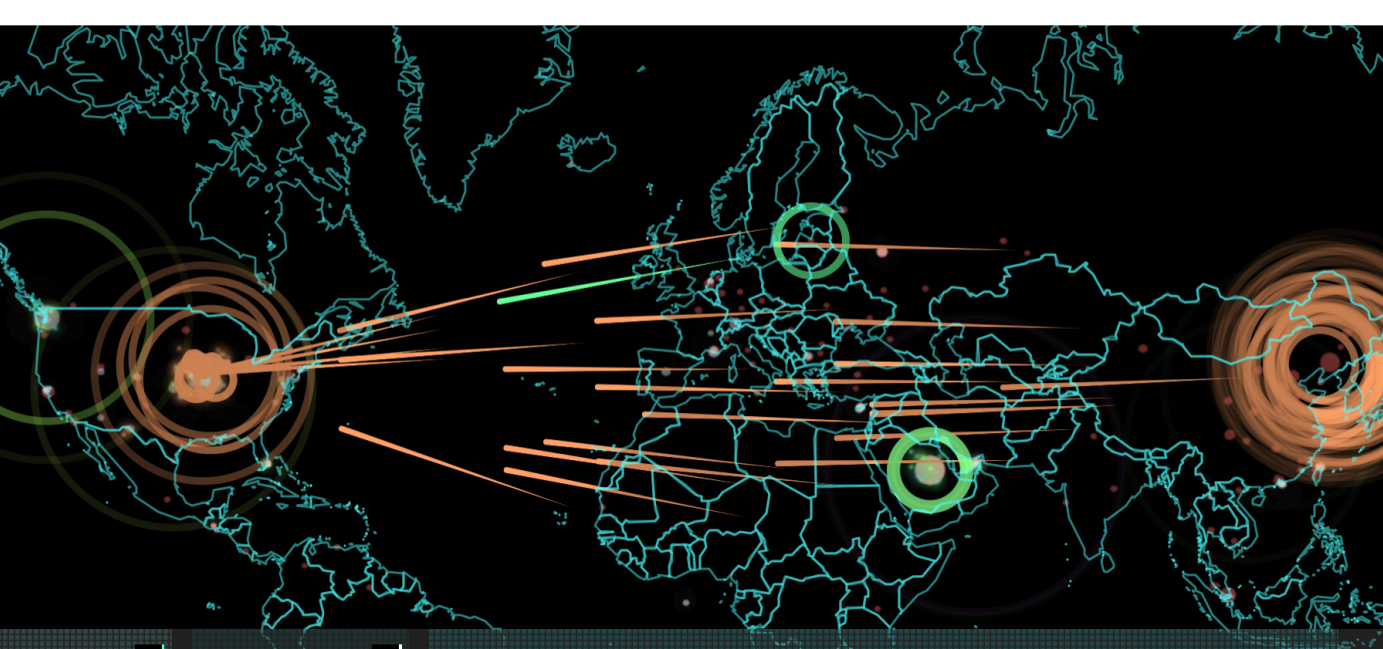
REFLECTIONS AND RECOMMENDATIONS FROM
THE ICT4PEACE FOUNDATION

Sanjana Hattotuwa, Barbara Weekes, Regina Surber & Daniel Stauffacher

GENEVA 2018
ICT4Peace Foundation



ORIGINS		ATTACK TYPES		ATTACK TARGETS		LIVE ATTACKS					
COUNTRY	#	PORT	SERVICE TYPE	#	COUNTRY	TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE
Germany	180	12199	unknown	198	United Arab Emi	09:47:36.928	Bsb-Service Gmbh	188.138.74.90	Cologne, DE	Dubai, AE	unknown
China	24	50864	unknown	88	United States	09:47:36.935	Bsb-Service Gmbh	188.138.74.90	Cologne, DE	Dubai, AE	unknown
Saudi Arabia	20	137	unknown	30	Saudi Arabia	09:47:36.940	Bsb-Service Gmbh	188.138.74.90	Cologne, DE	Dubai, AE	unknown
United States	13	50856	unknown	6	Bulgaria	09:47:37.102	Bsb-Service Gmbh	188.138.74.90	Cologne, DE	Dubai, AE	unknown





Getting down to business

Realistic goals for the promotion of peace in
cyber-space

A Code of conduct for Cyber-conflicts

Daniel Stauffacher, Chairman, ICT4Peace Foundation & Former Ambassador of Switzerland

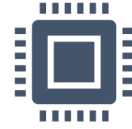
Riccardo Sibilis, Head of Cyber Threat Analysis, Swiss Armed Forces, Switzerland

Barbara Weekes, CEO, Geneva Security Forum

ICT4Peace Foundation

December 2011

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.



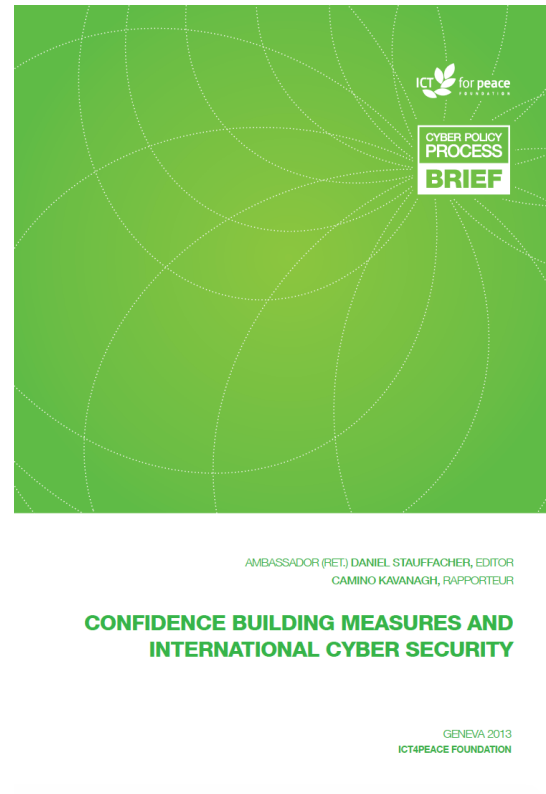
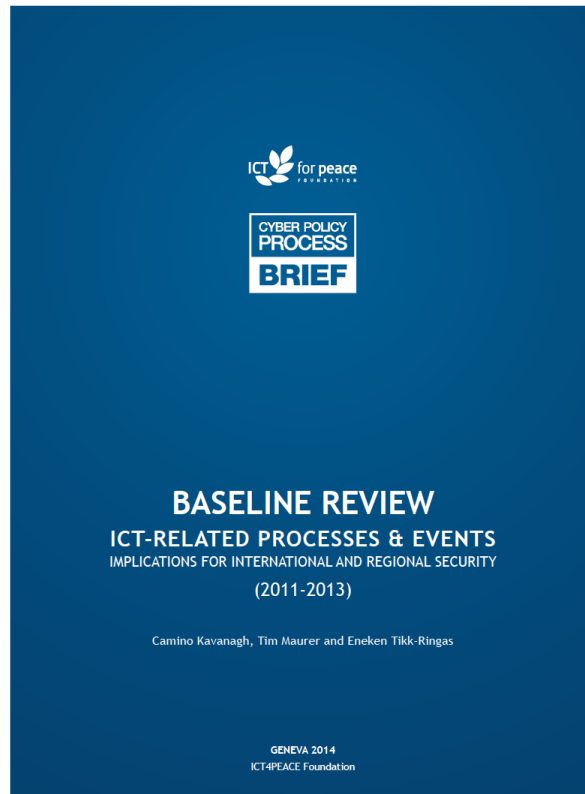
Damaging of a country's certain critical infrastructure: power, transport, financial sector etc. is possible.



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

The 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**



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

ICT4PEACE MATRIX: NATIONAL AND INTERNATIONAL GOALS AND MEASURES OF CYBERSECURITY

		Technical		Normative	
		Public Sector	Private Sector	Public Sector	Private Sector
National	<ul style="list-style-type: none"> National cybersecurity authority (incl. CERTs) Critical Infrastructure Protection 	<ul style="list-style-type: none"> Private Certs Private Critical Infrastructure Protection Big Companies SMEs Resilience 	<ul style="list-style-type: none"> National cybersecurity legislation Cyber Security Strategy 	<ul style="list-style-type: none"> Industry Standards Cybersecurity Governance Compliance Insurance 	
	<ul style="list-style-type: none"> CERT-CERT Cooperation Assistance in incident recovery Assistance in investigation and prosecution 	<ul style="list-style-type: none"> Assistance to Governments Solving technical flaws: Wannacry (MFST), Apple, Intel 	<ul style="list-style-type: none"> UN Charter and IL (ITU, Human Rights, LOAC/IHL, Cybercrime Conv. Voluntary norms (GGE, MSFT etc.) CBMs (OSCE, ARF) Security Council on ICT and Terrorism Global Culture of Cybersecurity 	<ul style="list-style-type: none"> Geneva Digital Convention (Microsoft) Microsoft norms proposals Siemens Charter Commitment to solve technical flaws Cooperation intra-Industry (start-ups) 	

RESILIENCE

PREDICTABILITY

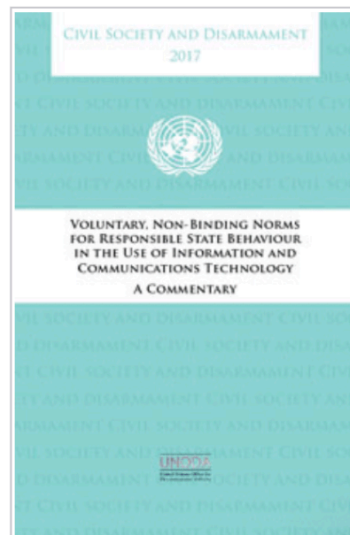
Institution and Capacity-Building

COOPERATION

ACCOUNTABILITY

Civil Society and Disarmament: 2017

Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary



Download PDF

[English](#)

Overview

This publication contains a commentary on the voluntary, non-binding norms of responsible State behaviour from the 2015 report of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. In an open call for comments, scholars, experts and enthusiasts were invited to submit recommendations, comments and guidance for understanding and interpreting the recommendations of the United Nations GGE. Many scholars and experts responded to this call and were involved in drafting this synthesis of views and perspectives.

Product Details

E.18.IX.3

ISBN:978-92-1-142326-6

eISBN: 978-92-1-363102-7

Publication date: December 2017

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

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



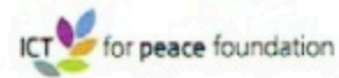
The ICT4Peace Foundation is honored to have been invited by the Government of Kenya to co-host the first regional training workshop in Africa (2 to 3 March 2015) on International Security and Diplomacy in Cyberspace with over 30 participants (Diplomats, Legal, Security and Technical Staff) from 12 African Countries, the African Union, and Civil Society Representatives. The workshop was co-chaired with Dr. Katherine Getao, Secretary, ICT Authority of Kenya. The Governments of Kenya, the UK, Germany and Switzerland supported the workshop course financially and with lecturers.

This new cyber security capacity building program was developed by the ICT4Peace Foundation as a direct follow-up to some of the recommendations tabled in the 2013 Report of the ["UN Group of Governmental Experts on](#)

Capacity Building
for International
Cybersecurity
Negotiations
Singapore October
2015



*Capacity Building for International
Cyber Security Negotiations
19 to 20 October 2015*



Confidence Building in Cyberspace: Constructive work by UN experts

United Nations

A/68/98*



General Assembly

Distr.: General
24 June 2013

Original: English

Sixty-eighth session

Item 94 of the provisional agenda**

**Developments in the field of information and
telecommunications in the context of international security**

**Group of Governmental Experts on Developments in the
Field of Information and Telecommunications in the
Context of International Security**

Note by the Secretary-General

Cybersecurity and Resilient Internet



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

PC.DEC/1106
3 December 2013

Original: ENGLISH

975th Plenary Meeting
PC Journal No. 975, Agenda item 1

DECISION No. 1106
**INITIAL SET OF OSCE CONFIDENCE-BUILDING MEASURES TO
REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE
OF INFORMATION AND COMMUNICATION TECHNOLOGIES**

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and

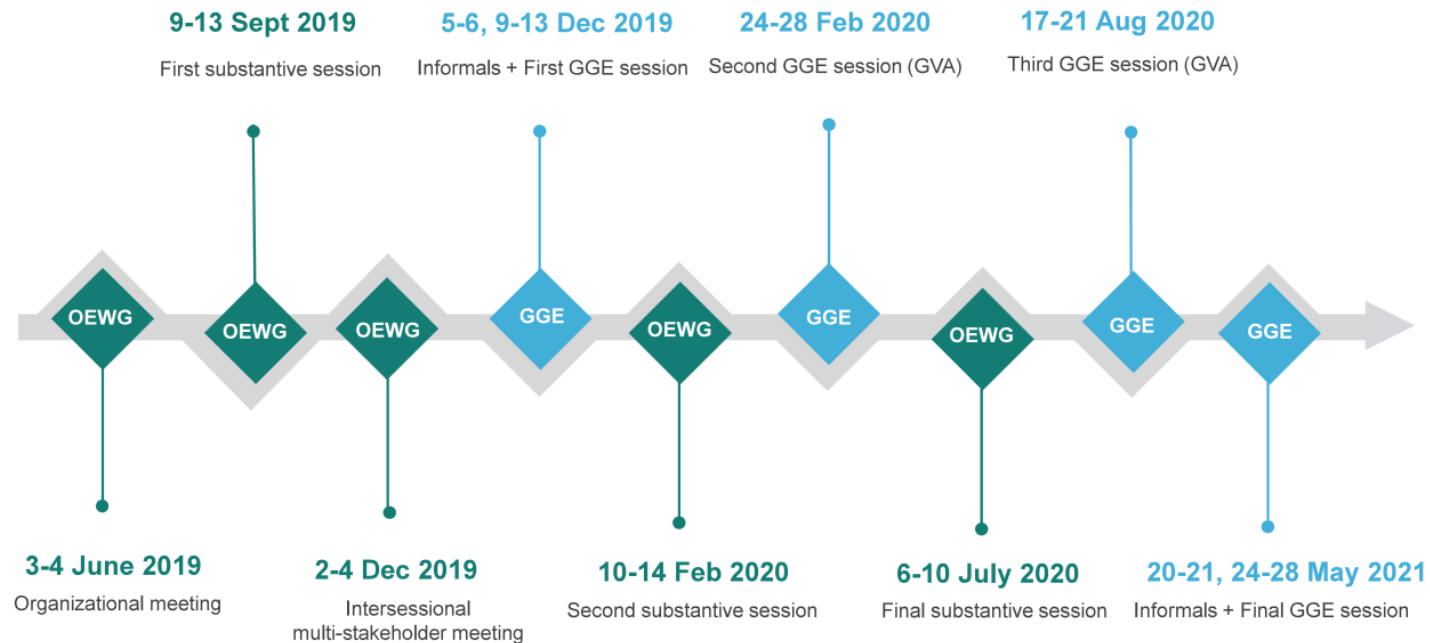
Developments in the field of information and telecommunications in the (

In December 2018, the General Assembly established two processes to discuss the issue of security in the use of ICTs during the period of 2019-2021, an Open-ended Working Group and a Group of Governmental Experts. Click on the below for more information.

Open-ended Working Group

Group of Governmental Experts

Tentative GGE and OEWG timeline (2019-2021)



← Activities / Norms of Responsible Behaviour and Confidence Building Measures (CBMs) for the Cyberspace

UN OEWG – UN Cybersecurity Negotiations launched in New York

🚩 Cybersecurity High-Level Policy Briefings, Norms of Responsible Behaviour and Confidence Building Measures (CBMs) for the Cyberspace

     share this page



🕒 11. SEPTEMBER 2019

On 13 September 2019 the first round of negotiations at the UN on Cybersecurity under the [UN Open Ended Working Group on Cybersecurity \(OEWG\)](#) took off in a positive spirit with general introductory statements by UN member states. The list of statements can be found [here](#). The



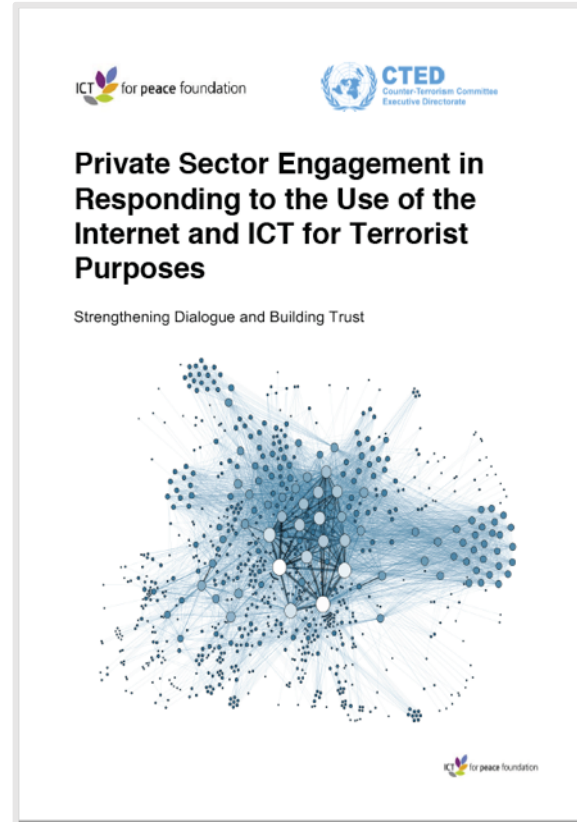
Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes

Strengthening Dialogue and Building Trust

April 2017

Presentation by Adam Hadley
adamhadley@ict4peace.org

We presented our summary report for Phase 1 at the UN in Dec



techagainstterrorism.org

Google: UN private sector engagement ICT For Peace

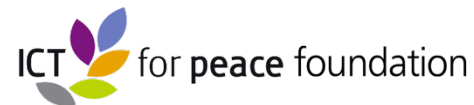
tech against terrorism



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*





**tech
against
terrorism**  **Global Internet Forum**
01 August 2017
San Francisco

The central graphic features the text "tech against terrorism" in a bold, black, sans-serif font. To its right is a network diagram icon consisting of several colored circles (orange, blue, green, purple) connected by lines. Further right, the event details "Global Internet Forum", "01 August 2017", and "San Francisco" are listed in a bold, black, sans-serif font.

Helping startups address the exploitation of their services





© 8. JANUARY 2018

Two UN Security Council Resolutions of December 2017 recognised the work of the ICT4Peace Foundation in launching the Tech Against Terrorism initiative in cooperation with [UN Counter Terrorism Executive Directorate \(UN CTED\)](#).

CHRISTCHURCH CALL



TO ELIMINATE TERRORIST
& VIOLENT EXTREMIST
CONTENT ONLINE

Christchurch Call

- Calls on Governments, Civil Society and Private Sector (Social Media Companies) “to eliminate terrorist and violent extremist content online”.
- <https://www.christchurchcall.com/index.html>

Governments

To that end, we, the Governments, commit to:

Counter the drivers of terrorism and violent extremism by strengthening the resilience and inclusiveness of our societies to enable them to resist terrorist and violent extremist ideologies, including through education, building media literacy to help counter distorted terrorist and violent extremist narratives, and the fight against inequality.

Ensure effective enforcement of applicable laws that prohibit the production or dissemination of terrorist and violent extremist content, in a manner consistent with the rule of law and international human rights law, including freedom of expression.

Encourage media outlets to apply ethical standards when depicting terrorist events online, to avoid amplifying terrorist and violent extremist content.

Support frameworks, such as industry standards, to ensure that reporting on terrorist attacks does not amplify terrorist and violent extremist content, without prejudice to responsible coverage of terrorism and violent extremism.

Consider appropriate action to prevent the use of online services to disseminate terrorist and violent extremist content, including through collaborative actions, such as:

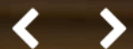
- Awareness-raising and capacity-building activities aimed at smaller online service providers;
- Development of industry standards or voluntary frameworks;
- Regulatory or policy measures consistent with a free, open and secure internet and international human rights law.

ICT4Peace input to Christchurch Call for Action by PM Jacinda Ardern at UN GA New York

🚩 AI disinformation and misinformation, Policy Research ICT, ICT4Peace in the Media, Publications, Responding to/preventing Violent Extremism using ICTs and the Internet, ICTs for the prevention of mass atrocity crimes, ICTs and Human Rights Protection, New media for crisis management and peacebuilding, Tech against terrorism



share this page





SANJANA HATTOTUWA
SPECIAL ADVISOR, ICT4PEACE FOUNDATION

Sanjana
Hattotuwa (Sri
Lanka)
TED Fellow,
Special Advisor,
IC4Peace

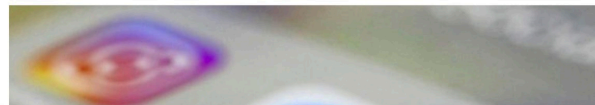
Full video & slidedeck of lecture: From Christchurch to Sri Lanka – The curious case of social media

AI disinformation and misinformation, Activities, Policy Research ICT, Capacity Building ICT, Advisory CS, Responding to/preventing Violent Extremism using ICTs and the Internet, ICTs for the prevention of mass atrocity crimes, ICTs and Human Rights Protection, New media for crisis management and peacebuilding, Big data, Tech against terrorism



17. JUNE 2019

On 20 May 2019, [Sanjana Hattotuwa](#), a Special Advisor at the ICT4Peace Foundation since 2006, gave a well-attended public lecture at the [University of Zurich](#) on the role, reach and relevance of social media in responding to kinetic and digital violence, including the potential as well as existing challenges around artificial intelligence, machine learning and algorithmic curation. The lecture was anchored to on-going doctoral research, data-collection and writing on the terrorist attacks in Christchurch, New Zealand in March and the Easter Sunday suicide bombings in Sri Lanka – Sanjana's home.



Artificial Intelligence and 'Fake News': Recording of public lecture

- Sanjana then looked at some factors, from the visual design of social media platforms to shifting markers of veracity of online content, that aided the spread and generation of misinformation. Three key effects of misinformation were flagged, and how such content was able to,
 - Amplify partisan frames
 - Drown out inconvenient truths
 - Seed distrust at scale
- <https://ict4peace.org/activities/policy-research/policy-research-ict/artificial-intelligence-and-fake-news-recording-of-public-lecture/>

Countering Violent Extremism (CVE) work in Afghanistan, Myanmar & the Balkans

- Work to strengthen civil society capacity on CVE
- Training independent journalists, including women, on social media as well as digital security
- Strategic communications for NGOs and CSOs in remote areas against violent non-state actors
- Risk assessment using open source intelligence frameworks
- Social media training, including using Facebook and Instant Messaging for content dissemination in austere contexts

Support of the UN's new plan of action against hate speech

- United Nations – Welcoming the United Nations Strategy and Plan of Action on Hate Speech, <https://ict4peace.org/activities/responding-to-preventing-violent-extremism-using-icts-and-the-internet/welcoming-the-united-nations-strategy-and-plan-of-action-on-hate-speech/>
- The Foundation's research into and work on the complex, fluid dynamics of hate speech, over a decade and across five continents, strongly complements the capture and submission of the problem space by the Secretary-General in his remarks at the launch of the strategy.

United Nations – Welcoming the United Nations Strategy and Plan of Action on Hate Speech

AI disinformation and misinformation, Responding to/preventing Violent Extremism using ICTs and the Internet, ICTs for the prevention of mass atrocity crimes, ICTs and Human Rights Protection



© 19. JUNE 2019

Image courtesy Vice

The ICT4Peace Foundation congratulates the Secretary-General of the UN on the [launch of the UN strategy and plan of action on hate speech](#). The Foundation's research into and work on the complex, fluid dynamics of hate speech, over a decade and across five continents, strongly complements the capture and submission of the problem space by the Secretary-General in his remarks at the launch of the strategy.

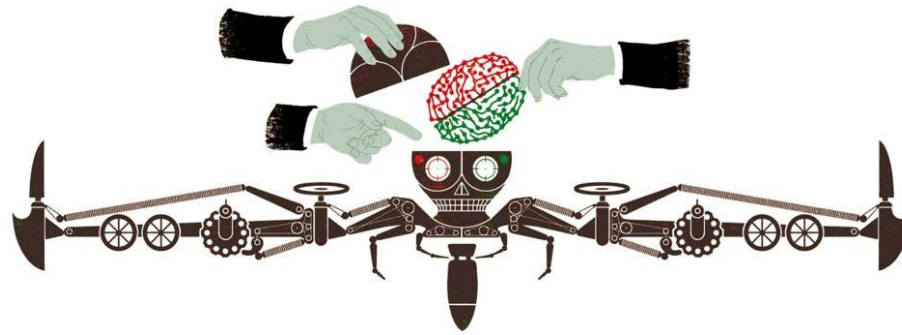
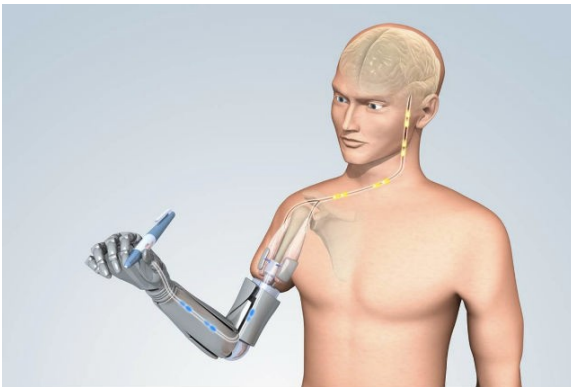
As far back as 2010, after meetings with the Office of the UN Special Adviser on the Prevention of Genocide, the Special Adviser on the Prevention of Genocide, Mr. Francis Deng and the Special Adviser on the responsibility to protect, Mr. Edward Luck, the Foundation published '[ICTs for the prevention of mass atrocity crimes](#)'. Some sections of the report, dealing with the challenges and opportunities of communications technology to prevent genocide, resonate deeply with the new

Artificial Intelligence: Autonomous Technology (AT), Lethal Autonomous Weapons Systems (LAWS) and Peace Time Threats

By Regina Surber, Scientific Advisor, ICT4Peace Foundation and the
Zurich Hub for Ethics and Technology (ZHET)

Artificial Intelligence

- Research field with rapid progress
- Currently: Weak AI – performance in a specific area. (vs. strong AI)
- Highly ‘intelligent’ -> ‘autonomous’: unpredictability, loss of human control and responsibility?
- Inherently dual-use



Lethal Autonomous Weapons Systems

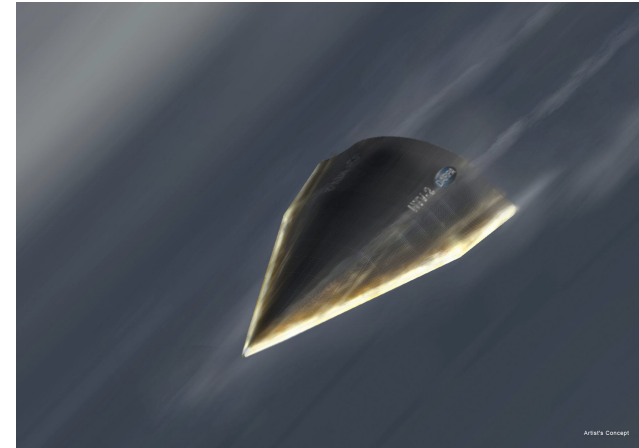
ICRC 2016: *Identify, select, track, attack target with little or no human involvement*



Samsung TECHWI SGR-A1
Source: Samsung TECHWI



Dassault nEUROn
Unmanned Combat Aerial Vehicle
(UCAV) Source: Dassault Aviation



Dassault nEUROn
Unmanned Combat Aerial Vehicle
(UCAV) Source: Dassault Aviation



X-41 ?
Source: Space.com

Peace-Time Threats

1. AI-enabled technology and mass disinformation
2. AI-enabled technology in the justice system
3. AI-enabled technology in light of resource-scarcity during times of crisis
4. New (artificial) species – a threat for humanity?
5. ...?

United Nations Convention on Certain Conventional Weapons

- Informal discussions
20014- 2016; Group of
Governmental Experts
2016
- 2018 Report with
emerging Principles
- Legality
- (Working) Definitions



Meeting of the High Contracting Parties to the CCW,
Geneva 2014. Source: GICHD.

HUMAN RIGHTS

- The protection of human rights – particularly the freedom of expression and of opinion - has figured strongly in discussions and debates surrounding cyberspace.
- A major milestone was reached when the UN Human Rights Council adopted a Resolution in 2012 'affirm[ing] that the same rights that people have offline must also be protected online.
- A series of events led to this affirmation. For example, in May 2011, the G8 adopted the Declaration on Renewed Commitment for Freedom and Democracy. Noting that the Internet poses a 'unique information and education resource,' the Declaration acknowledges its potential as a tool to promote human rights, freedom and democracy while stressing the importance of openness, transparency, and freedom as the essential driving forces behind the success and development of the Internet.

Statements on disinformation by David Kaye

- Hate speech: UN experts make joint call for action by states and social media firms,
<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25037&LangID=E>
- JOINT DECLARATION ON FREEDOM OF EXPRESSION AND “FAKE NEWS”, DISINFORMATION AND PROPAGANDA,
<https://www.osce.org/fom/302796?download=true>
- Freedom of Expression Monitors Issue Joint Declaration on ‘Fake News’, Disinformation and Propaganda,
<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E>

Key recommendations to the HLP on Digital Cooperation

The ICT4Peace Foundation is working to promote Digital Human Security, extending the concept of Human Security (UNDP 1994) to encompass technological issues that threaten humanity, and to consider the full impact of technology from fake news to the latest developments in AI.

Crisis Information Management:

1. **Continue to implement and review periodically the UN Crisis Information Management Strategy CiMS (A/65/491), in particular the recommendations of the last stock-taking exercise in February 2018.**
2. **Prepare for the future through scenario planning.** Conduct future scenario planning exercises to ascertain if the UN system is thinking far enough into the future.
3. **Better manage existing knowledge and information.**
4. **Become an anchor of ethics in an AI world.**
5. **Champion the truth.** In a post-truth world, the UN needs to champion accurate, responsible and impartial sources of information and media for use in Crisis information Management (CiM) and beyond.
6. **Embrace quantum computing (QC).** How can the UN adapt current QC frameworks to improve efficiencies and effectiveness of responses to problems the UN system faces, including political and socio-economic issues?

Social media:

1. **Challenge simplistic conflict analyses that blame social media.** Technology is an enabler for whatever an actor intends to do and the complexity of violence, its generation and transformation, should not be viewed through a single lens.
2. **Recognize that basic principles of communication are essential on social media and develop visual types of social media content.** The UN family needs to embrace this transformation in content, in order to bring about change they want to see.
3. **Strengthen media literacy, social media security and communications planning.**
4. **Build civil society capacity in social media and develop local approaches to misinformation and hate speech.**
5. **Design social media to harness our "better angels."**

Key recommendations to the HLP on Digital Cooperation

Artificial Intelligence:

1. **Create a UN level body for technology and AI** with the tasks of ensuring responsible technological research and discussing peace and security implications of emerging technologies
2. **Integrate the use of autonomous cyber weapons and autonomous weapons during law enforcement into international discussions.**
3. **Look beyond the issues of AI and Autonomous Weapons Systems (LAW) but consider also the short, medium and longterm "Peace Time Threats" for Society.**
4. **Foster a public discussion of the human-machine analogy and further the dialogue between tech experts, civil society and government.** Technologists must learn to transfer their expert knowledge in a practical way. This could be enhanced if courses were included in university curricula.
5. **Launch a debate on property rights on source codes of AI and AT software.**
6. **Encourage the increased engagement of civil society, including the private sector and academia, on the questions of human control of and responsibility for technological outcomes.**

Our team

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



Kristina Rintakoski

Board Member



Juliana Rotich

Board Member



Kamal Sedra

*Senior Technical
Advisor*



THANK YOU
danielstauffacher@ict4peace.org