ICT for peace foundation

HIGH-LEVEL PANEL ON DIGITAL COOPERATION

REFLECTIONS AND RECOMMENDATIONS FROM THE ICT4PEACE FOUNDATION

Sanjana Hattotuwa, Barbara Weekes & Daniel Stauffacher

GENEVA 2018
ICT4Peace Foundation

ICT4Peace Publishing, Geneva. November 30, 2018
Copies available from www.ict4peace.org

HIGH-LEVEL PANEL ON DIGITAL COOPERATION

REFLECTIONS AND RECOMMENDATIONS FROM THE ICT4PEACE FOUNDATION

Sanjana Hattotuwa, Barbara Weekes & Daniel Stauffacher

ICT for peace foundation

HIGH-LEVEL PANEL ON DIGITAL COOPERATION

REFLECTIONS AND RECOMMENDATIONS FROM THE ICT4PEACE FOUNDATION

The ICT4Peace Foundation is pleased to present for the consideration of the High-level Panel on Digital Cooperation some insights, observations and recommendations based on over ten years of a close, multi-level, multi-sectoral association with the United Nations system. Of relevance to the HLP could be several specific foci of the Foundation's output.

What follows is a snapshot of themes and key outputs around a few core work-streams. We are ready to assist the HLP in their vital work moving forward to establish, strengthen and widen the application of what it flags as necessary for the UN to more fully respond to needs and challenges in the 21st Century.

The road to Digital Human Security: What values and principles should underpin cooperation in the digital realm?

Recalling in particular the Universal Declaration of Human Rights, the ICT4Peace Foundation's belief in the power of technology to engender, engineer and envision peace is founded in the mission and enduring mandate of the United Nations. As the custodian of Paragraph 36 of the World Summit on Information Society (WSIS[1]), the Foundation was one of the first in the world to support the UN's vision at seeing a just, peaceful world through the strategic, sustained use of technology. We have since our inception observed a world that is quick to take advantage of technologies for violence, war and the pursuit of parochial, partisan ends. Our response, throughout the years, is anchored to our founding mission and vision – that technology is only as good as those who wield it.

1 http://www.itu.int/net/wsis/docs/geneva/official/dop.html

In 1994 the UNDP Human Development Report presented the concept of security as linked to humans rather than geographical entities and to development instead of weapons. The concept of human security included freedom from fear and freedom from want. Human security encompasses food, a safe place to live, healthcare, economic well-being and education. It is now time to extend this to encompass technological issues that threaten human security; to consider the full impact of technology on the individual from fake news to the latest developments in AI.

For years, we have supported the work of the UN family and championed **ethics, human rights, international norms and standards** as pillars of collaboration and coordination that must undergird peaceful uses of technology. This now extends to the prevention of mass atrocity crimes[2], cybersecurity, artificial intelligence, countering violent extremism online as well as combatting misinformation and disinformation.

Our engagement with OHCHR's important mission has consistently been to strengthen its effectiveness in a complex world, and help those in charge of rapid response and commissions of inquiry make better use of tools that can help in information gathering, sharing, dissemination and archiving.

Our pioneering work with all the leading peacekeeping and humanitarian actors in the UN family, since 2008, is founded on the spirit of information sharing within and between UN actors as well as with a larger community of first responders. As early as 2010, just after the catastrophic earthquake in Haiti, we stressed the urgent and enduring need for:

1. Pre-planned information-sharing policies robust enough to handle severe crises in a timely manner. This includes policies to leverage crisis-related information generated from outside the UN system and the development of robust data models and data dictionaries that can be shared on demand.

2. An emphasis on standards-based information capture and exchange.

3. Harmonisation of significant variance in agency approaches to, and capacities of, information management during crises, including human resource management and data-sharing policies.

Also as far back as 2010, the values and principles of collaboration we supported and helped introduce at the UN were recognised by the General Assembly[3] and the then

2 https://ict4peace.org/activities/policy-research/policy-research-ict/icts-for-the-prevention-of-mass-atrocity-crimes/

3 https://ict4peace.org/updates/report-of-the-un-secretary-general-underscores-crisis-information-management-strategy

recently established Office of Information and Communications Technology (OICT[4]). We helped engineer the world's first machine-readable standard for information exchange especially vital in humanitarian response[5], again propelled by the belief that information hoarding was inimical to saving lives.

In fact, our work over 10 years of collaboration with the UN[6] across a number of continents and contexts, validates the HLP's *raison d'etre* at this critical juncture, where the UN's mission, vision and mandate need to be realigned with global and local challenges that test its resilience and effectiveness in profoundly new ways.

None of these are new values or principles. They are well-known. The challenge is in their unequal application and spread. With the HLP's timely and important input helping the UN Secretary-General's strategic vision, the Foundation sincerely hopes that this report can provide some guidance, based on our expertise, to help steer conversations on the role, reach and relevance of technology in strengthening justice, peace, democracy, development and human rights.

Crisis Information Management including countering violent extremism, disinformation and misinformation online

Our work on Crisis Information Management (CiM) with the UN family started in 2008. Invited by the UN Chief Information Technology Officer (UNCITO), ICT4Peace undertook a first ever stocktaking exercise of UN Crisis Information Management Activities, Capabilities and Best-Practice. All of the organisations in the Chief Executive's Board (CEB) participated in the stocktaking exercise, including all of the UN Agencies, Funds and Programmes, the Departments of the UN Secretariat, and other members of the broader UN System. The Stock-taking Report is online[7].

In the Status Report on implementation of the Information and Communications Technology strategy for the United Nations Secretariat, a 2010 report of the Secretary-General to the General Assembly (A/65/491), it is noted that the Crisis Information

4 https://ict4peace.org/updates/united-nations-core-ict-strategy-incorporates-crisis-information-management

5 https://ict4peace.org/activities/welcoming-hxl-version-1-0-a-breakthrough-in-humanitarian-information-exchange/

6 https://ict4peace.org/activities/the-crisis-information-management-strategy/

7 https://ict4peace.org/wp-content/uploads/2010/05/Interim-Report-Web-Version1.pdf

Management Strategy is based on the recognition that the United Nations, its Member States, constituent agencies and non-governmental organisations 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 ICT4Peace Foundation in cooperation with UN CITO, subsequently facilitated annual retreats of the Crisis Information Management Advisory Group (CiMAG) from 2008 to 2016, to support and facilitate the implementation of the UN Crisis Information Management Strategy (CiMS). Members of CiMAG include inter alia: UN CITO, Office of SG, OCHA, DPKO, DFS, DPA, UNHCR, WFP, OHCHR, UNDP, UNICEF, DSS, UNFPA, PBSO, ICT4Peace.

In 2017, there was broad recognition that a unique opportunity existed under the leadership of the new UN SG and senior staff including ASG Hochschild, to push forward the core tenets of the Crisis Information Management Strategy. In the second half of 2017, ICT4Peace, supported by the Government of Sweden, was invited by ASG Hochschild to carry out a second rapid stocktaking on capacities and capabilities around crisis information management (similar to the one in 2008).

This process involved face to face meetings as well as an online questionnaire. The questionnaire aimed to get respondents, mostly from the Crisis Information Management Advisory Group (CiMAG) to reflect on the CIM framework which had four major components: information architecture, technology development, stakeholder management, and capacity building. These pillars were supposed to influence governance, funding, evaluation and incrementalism in the crisis information management domain.

An informal and draft report by the CIMAG members on findings and recommendations of the CIMAG Retreat is online[8]. All the documents and public facing output from the CiMAG process since 2008 are also online[9].

8 https://ict4peace.org/cimag-meeting-note-to-asg/

9 https://ict4peace.org/activities/the-crisis-information-management-strategy/

Recommendations anchored to the 2017/2018 Stock-taking Report pertinent to the HLP are:

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. Extra- terrestrial, terrestrial, subterranean, oceanic, tectonic and technological Black Swan events should be embraced in these exercises. For example, a discussion around the end of Net Neutrality and what a tiered Internet will look like and cost, as well implications for the UN and IM in particular.

3. **Better manage existing knowledge and information.** Better management and use of what is present and known, instead of indiscriminate investments to gather additional information.

4. **Become an anchor of ethics in an AI world.** Ethics around innovation, including in particular machine learning (ML) and AI driven decision-making are of increasing importance – what are the overarching considerations in pushing for AI if, without governance, it can be used for hate, hurt and harm? How can the UN emerge as a global ethics anchor in the AI space? What can the UN do to provide algorithmic oversight on ethical grounds, as well as ensuring rights and privacy of individuals aren't violated because of big data investments?

5. **Champion the truth.** In a post-truth world, images, video and audio that are doctored are (digitally and for human perception) indistinguishable from factually accurate content (e.g. 'Photoshop for Audio', Unsupervised Image-to-Image Translation Networks, and real time video manipulation). How can the UN champion accurate, responsible and impartial sources of information and media for use in CiM (and beyond)?

6. **Embrace quantum computing (QC).** How best to embrace quantum computing (QC), which is not yet really on the UN's radar? Can current QC frameworks be adapted to improve efficiencies and effectiveness of responses to problems the UN system faces, including political and socio-economic issues?

The use of social media: fragile democracies, civil society and international humanitarian actors[10]

The Foundation has for many years worked at the forefront of applied social media research, focussing on the impact new technologies have on fragile democracies, polity and society. In recent years, this work has embraced digital-security training for activists, human rights defenders and journalists at risk, misinformation and disinformation research, constructing and implementing countering violent extremism initiatives online, research into algorithmic manipulation of social media (included "fake news") and other related domains. The Foundation's experience is cross-cutting, and across austere contexts, ranging from Afghanistan to Myanmar.

Key recommendations on Social Media:

1. **Challenge simplistic conflict analyses that blame social media.** There is no easy or "one" solution to protracted conflict and systemic discrimination. Successive governments across the world have flagged Facebook and social media as the sole or primary progenitors of violence, ignoring the fact that governments themselves have done little to uphold the Rule of Law or address the root causes. 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. **Embrace the transformation and use of social media, and develop visual types of social media content.** Even as technology changes, basic communications strategies have enduring value and resonance. However, the UN family needs to embrace the move to social media, in order to bring about the change they want to see. The most viral content on Facebook and Twitter are anchored to photos, memes and short form video. Facebook Live Video generates hundreds of thousands of views and around key events, runs into the millions. Live coverage over Facebook is now a primary vector of news and information for a young demographic. Content that is emotive, anchored to slang and speech forms, geared for mobile screen dimensions, is subtitled to enable muted viewing are some of the strategies employed by the most engaged accounts on social media. The UN family needs to study and emulate.

10 https://ict4peace.org/activities/impact-of-social-media-in-elections-a-policy-brief/

3. **Strengthen media literacy, social media security and communications planning.** A little knowledge combined with minimal security awareness can be very dangerous. Haphazard and ill-advised forays into social media can result in: increased risk, exposure, unwanted scrutiny, denial of service attacks on critical online infrastructure, becoming the target of bots and trolls, doxing and breaches of privacy, increased barriers around messaging, content generation and promotion.

4. **Build civil society capacity in social media and develop local approaches to social media, misinformation and hate speech.** Investment in social media by civil society is still regarded as optional or peripheral to projects dealing with governance, democracy, electoral systems, accountability, reconciliation, peacebuilding and media. Unless the strategic adoption and timely adaptation of social media is mainstreamed into civil society programmes, bad-faith actors with a vested interest in leveraging social media to divide and destroy, will continue to have the upper-hand. Misinformation spreads fast on social media and the speed and scale have increased with the greater adoption of social media by millennials. This is compounded by an enduring lack of media and information literacy. It is important to study and understand what drives the worst of the hate, and also know when and when not to engage. Misinformation must be handled with care, and in line with robust research done globally as well as locally around how best to operationalise counter-speech, fact- checking and the debunking of rumour. Social media is a dynamic environment, where platform, app, device, language, age and location all play a role in how a particular person, event, process, idea or institution is discussed. Knowing this, and doing the research, before producing and promoting one's own content is vital. It is also important to not just focus on a single dominant language but rather debate and clarify in other dialects or languages, which may have very different foci and frames of reference.

5. **Design social media to harness our "better angels".** The challenge for civil society and liberal democracy is to work with leading social media companies to connect with citizenry in a manner that harnesses our better angels. To promote a cohesive vision of a peace with justice, a future that acknowledges the past, a reconciliation pegged to accountability and a society that values democracy, decency and human dignity.

Artificial Intelligence, Lethal Autonomous Weapons Systems and Peace Time Threats and implications for the UN

Years of research and four years of discussions of LAWS within the UN CCW have not lead to terminological clarification of "autonomy". Instead opinions on the scope and content of the term 'autonomy' or AT have become even more diverse. A fixed definition of 'autonomy' for technological artefacts could lead to a clear definition of LAWS within the GGE, which in turn could encourage a potential outcome of the UN discussions (e.g. Code of Conduct or norms for responsible State behaviour). However, the endeavour to minimize risks of AI and AT must not lose focus due to definitional questions regarding LAWS but rather concentrate on binding principles for responsible AI research. This alternative track would take into account the fact that 'autonomy' for technological artefacts, e.g. LAWS, can and should be regarded as a proxy term for the loss of human control and responsibility for outcomes of technological processes.

Principles guiding AI research could require programmers and engineers to develop **only** technological artefacts whose outcomes will stay controllable for humans, and for which the latter would always bear responsibility. Initiatives of professional organizations as well as representatives of the private sector have developed several lists of principles for responsible and ethical research on AI and autonomy. It would be advisable to bundle those principles and create an international body that would supervise and assist with coordination and implementation.

An open discussion must be encouraged with all stakeholders on whether or not humanity accepts that technology is already crossing a threshold after which its creations might be uncontrollable for humans. The UN CCW's debate on LAWS has brought this crucial moment into the public spotlight. However, AI is much more than just its representation in LAWS. If we really want to look after the future of humanity, it is a prerequisite to gain a holistic understanding of all the peace and security implications of AT and emerging technologies. For a purposeful discussion of this broader question, a new international forum is needed.

Another key area that needs to be addressed is the use of autonomous cyber weapons and autonomous weapons during law enforcement operations. These are currently beyond the mandate of the CCW discussions, yet they reflect the seriousness of the risk of weaponized AT. If the international community wants to prove its serious commitment to the issue of emerging technologies, the use of autonomous cyber weapons and autonomous weapons during law enforcement operations must be included in international discussions.

The broader international discussion of AI, must also include an assessment of the peace-time threats of not-weaponized AT, such as mass dis- and misinformation as well as autonomous profiling and citizen control. Peace and security implications of emerging technologies including i.a., AI, biotechnology, 5G radiation, and molecular nanotechnology are also of critical importance. Threats for humanity stem from many more technological endeavours, whose risks are yet to be analysed. A fixed body of experts at the UN level should take on discussions of the peace and security implications of all emerging technologies and the peace and security implications of not-weaponized AT during peace-time.

Moreover, the international debate on LAWS contains the unexamined assumption of a human-machine analogy. However, the view that hvvuman qualities can be reproduced in machine should not be accepted unconditionally. As long as science cannot fully reveal the physical representation of human intelligence, consciousness, and decision-making processes in the human brain, self-protection should force us to acknowledge human distinctiveness. The fact that 'being human' is unquantifiable for science must not mean that human distinctiveness does not exist. We have a duty to preserve an assumption of this distinctiveness by limiting potential technologies that could challenge it or even wipe it out.

One way of preserving an understanding of the distinctiveness of 'being human' is through a careful use of language. Software or machine 'autonomy', 'intelligence' or 'agency' are terms that are very problematic in this sense. A premature heroization of technology could be prevented by introducing distinct terms. By using a term such as, e.g., 'artefact with *cognitive functions*' instead of 'intelligent agent', the fact that the machine is performing a *function* would be highlighted. This would set a clear boundary to being 'human and intelligent', as humans are not only performing a function, but are always an end unto themselves. Moreover, the term 'artefact' would point out its objective character as opposed to 'agent'.

In addition, the view of the inevitability of AT and LAWS, which, unfortunately, reigns in the minds of many must be challenged. The use of any software that could potentially interfere with a citizen's privacy or physical integrity could and should be regulated by a democratic process. This is a difficult demand or expectation but it is important to start thinking and planning for this future today.

An introduction of software codes into a legislative process would require a creation of a constant policy-technology interface through, e.g., fixed state departments for technology and AI. A constant dialogue between tech experts and policy-makers through institutional integration could limit the risk that programmers and policy-makers could palm off the responsibility of 'autonomous' systems' 'immoral' outcomes to each other. Further, such an idea would require source codes to be publicly

accessible, for which deeply considered answers to the question of property rights of source codes of autonomous and other systems are a prerequisite.

Humanity is striding into a future where machines and software will have an unprecedented role in almost all aspects of our lives. Moreover, future technology may have an immense potential for humans to define what they want to become. If we want to navigate wisely through a future that we might share with artefacts with cognitive abilities, we need to discuss some serious questions on 'autonomy', 'responsibility,' 'privacy' and 'identity'– and we have to do it now. These thoughts represent a small contribution to those profound challenges.

Key recommendations on AI and AT:

1. A creation of 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, i.a. AI and AT, biotechnology, 5G, molecular nanotechnology. This body would also set principles for responsible research in the above-mentioned scientific fields and coordinate implementation.

2. An inclusion of autonomous cyber weapons and autonomous weapons during law enforcement into international discussions. The former could be integrated into the GGE on LAWS, and the latter could be taken up by the Human Rights Council.

3. **Look beyond the issues of AI and Autonomous Weapons Systems (LAW) and consider also the short, medium and long term "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.

5. Launch a debate on property rights for 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.

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

In December 2015[11] the UN Counter Terrorism Executive Directorate (CTED) invited ICT4Peace to help promote a dialogue at the UN Security Council between Governments and Tech Companies, in particular social media companies to prevent the use of ICTs for terrorist purposes, while respecting human rights and freedom of speech.

In April 2016 UN CTED and ICT4Peace formally launched a joint project[12] on technology sector engagement in responding to terrorist use of ICTs with the objective to deepen understanding of current industry responses to terrorist use of their products and services, particularly with regard to content and-operational related issues and identify practices and experiences. An overview of the implementation of this project is online[13].

In December 2016 UN CTED and ICT4Peace launched the first comprehensive report 'Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust[14]'.

In May 2017 ICT4Peace introduced the UN CTED-ICT4Peace "Tech Against Terrorism" Project at the 2017 OSCE-wide Counter-Terrorism Conference in Vienna[15], and in August 2017 UN CTED and ICT4Peace hosted the U.S. launch of the Global Internet Forum to Counter Terrorism (GIFCT[16]) at Swissnex in San Francisco. In November 2017 UN CTED and ICT4Peace launched the "Knowledge Sharing Platform "Tech against Terrorism[17]".

11 https://ict4peace.org/activities/ict4peace-at-un-special-sessions-on-preventing-abuse-of-ict/

12 https://ict4peace.org/activities/un-and-ict4peace-engage-with-private-sector-on-responding-to-terrorist-use-of-ict/

13 https://ict4peace.org/activities/tech-against-terrorism/?load=all

14 https://ict4peace.org/activities/private-sector-engagement-in-responding-to-the-use-of-the-internet-and-ict-for-terrorist-purposes-strengthening-dialogue-building-trust/

15 https://ict4peace.org/activities/ict4peace-presents-tech-against-terrorism-project-at-osce-in-vienna/

16 https://ict4peace.org/activities/ict4peace-and-un-host-launch-of-new-global-internet-forum-with-tech-companies-in-san-francisco/

17 https://ict4peace.org/activities/ict4peace-and-un-cted-launch-knowledge-sharing-platform/

In January 2018 two UN Security Council Resolutions[18] recognised the work of the ICT4Peace Foundation in launching the Tech Against Terrorism initiative in cooperation with UN Counter Terrorism Executive Directorate (UN CTED).

Key recommendations on Tech against Terrorism:

1. **Deepen understanding and awareness of terrorist use of private sector products and services**
2. **Encourage and develop appropriate response mechanisms to terrorist use of private sector products and services**
3. **Encourage sharing and use of best practices.**

Cybersecurity and capacity building for LDCs

An open, free and sustainable internet cannot be taken for granted. Solutions to some of these new challenges are being generated as much by states (e.g. developing norms of state behavior and confidence building measures (CBM's) as by non-state actors, by building for instance new cyber security standards with the help of the new intermediaries (e.g. ISPs), business companies and consumer organizations. ICT4Peace experts have been working on Cyber Security since 2007 and calling since 2011 for more engagement by States, Private Sector and Civil society to address the new and emerging serious challenges posed to the cyberspace and called e.g. for a code of conduct in June 2011. Since then ICT4Peace has put together a small team of international lawyers, security specialists and a disarmament Ambassador to carry out research and advocacy, advise Governments, participate in Track Two Negotiations and important international governmental meetings such as the UN Governmental Group of Experts, OSCE Working Group on Confidence Building Measures for the Cyberspace (member of Swiss Government Delegation), London-Seoul-Hague Conference. An important example of recognition of the work of ICT4Peace is the inclusion of ICT4Peace's Report on Confidence Building Measures for the Cyberspace, the Baseline Review Document and the report on the Role of Civil Society in Cybersecurity discussion (9) in the Report of the US Library of Congress' Congressional Research Service's list of authoritative publications on Cyber Security issues. A further example of the recognition of the work of ICT4Peace

18 https://ict4peace.org/activities/un-security-council-recognises-ict4peaces-work-with-the-united-nations/

and its achievements, is found in the final outcome document of the London - Seoul Conference on Cyberspace.

Given the accelerating deterioration of international relations, including global cyber relations, it has become most urgent that international norms of responsible state behaviour be adopted and adhered to by all states and non-state actors. The ICT4Peace Foundation sponsored the first Global Commentary on "Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology" published by the United Nations in April 2018. This process was started in July 2017 when ICT4Peace co-launched a global call for Comments by scholars and practitioners, on how to implement the United Nations' Recommendations on Responsible State Behaviour in Cyberspace.

Importantly many states, especially developing countries and LDCs still lack sufficient capacity to protect their ICT networks and to engage in bilateral, regional and global cooperation at the technical and diplomatic level and to learn about concrete threats and respond effectively to them. The lack of such capacity can make national institutions and critical infrastructures (power, telecom, hospitals, transport and financial) vulnerable and can hamper economic and social development. It can make a country even an unwitting haven for malicious actors, which negatively impacts the global ICT network on the whole. It is often said, that the global ICT network "is only as strong as its weakest link".

Capacity building in cyber security policy, strategy and diplomacy plays an essential role in:

- States engaging in international cooperation and negotiations (as outlined in the 2013 and 2015 GGE reports on norms and CBMs (UN GGE proposed Norms of Responsible State Behaviour, OSCE and ASEAN adopted Confidence Building Measures (CBMs) for the promotion of a secure and peaceful cyberspace).
- enabling countries to secure their ICT infrastructure for economic and social development and,
- strengthening the global ICT network to ensure peaceful use for economic and social development.

Since 2014 and with the support of the Governments of the UK, Germany, Switzerland, Netherlands, Colombia, Kenya, Singapore, Australia and New Zealand, the ICT4Peace Foundation has carried out a series of Capacity Building workshops for Latin American Countries (in Bogota in cooperation with OAS), for African Countries (AU, Addis Ababa), for East African Countries (Nairobi), for ASEAN Countries (Singapore), Europe (GCSP, Geneva), for OSCE Field staff (Vienna), for Cambodia, Laos, Myanmar,

Vietnam (CLMV countries) in Laos, Vientiane; Hanoi, Vietnam, for ASEAN Countries Thailand and in Singapore. The General Objectives of the Workshops are:

- Better awareness of issues of international cyber security by public officials and diplomats (international law and norms, CBMs and international cooperation as outlined in the UN GGE Reports, by ASEAN, OSCE, AU, OAS etc.);
- Feedback from the Regions to the international cyber security dialogue and discourse;
- Better mutual understanding of related concepts, norms and measures, strengthened and possibly institutionalized cooperation among participating countries;
- Exchange of concerns, best practices, policies and institutional arrangements in the field of cyber security;
- A network of alumni, lecturers and experts familiar with the international cyber security challenges and processes and willing to support the goals of implementing and universally promoting inter alia the UN GGE guidance on norms and CBMs.

Key recommendations on cybersecurity and LDC capacity building:

1. **Support an open, secure, stable, accessible and peaceful cyberspace.**
2. **Participate in the setting up of an independent network of organisations engaging in attribution peer-review.** In order to curb adverse effects stemming from the misuse of offensive cyber capabilities, effective, technically mature and above all trustworthy attribution is indispensable. https://ict4peace.org/activities/trust-and-attribution-in-cyberspace-an-ict4peace-proposal-for-an-independent-network-of-organisations-engaging-in-attribution-peer-review/
3. **Support the recognition of the concept, that cybersecurity has become a fundamental development issue and a critical responsibility of all stakeholders including government, civil-society, business and academia.**
4. **Support capacity buil ding in cyber security policy, strategy and diplomacy in Developing Countries and especially LDCs. Also support the building of CERT (Computer Emergency Response Teams) capabilities in Developing and Emerging Economies.**
5. **Work to strengthen relevant international standards in cyberspace.**

6. **Continue work via the UN GGE, but also with OAS, ASEAN, AU, OSCE to promote norms of responsible behaviour and confidence-building measures for the cyberspace.**

Contact:
Daniel Stauffacher
President
danielstauffacher@ict4peace.org

About ICT4Peace Foundation

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.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with the publication of a book by the UN ICT Task Force on the practice and theory of ICT in the conflict cycle and peace building in 2005 and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation