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.**

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:

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 Cyberscurity has become a fundamental development issue and statehood building, and a critical function and responsibility of any state, but also civil-society, business, academia.**

Key recommendations to the HLP on Digital Cooperation

4. Support capacity building 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.