10th International Conference on the New Haven School pf Jurisprudence and International Law

Emerging Threats in Cyberspace

Daniel Stauffacher

ICT4Peace Foundation

Hangzhou, 31 May – 1 June 2019

ICT for peace foundation

ICT for peace foundation

ICT4Peace is a policy and action-oriented international Foundation. Our purpose is to save lives and protect human dignity through Information and Communication Technology.

We promote cybersecurity and a peaceful cyberspace through international negotiations with governments, companies and non-state actors. We also explore and champion the use of ICTs and media for crisis management, humanitarian aid and peace building.

To learn more about our activities and projects: **www.ict4peace.org**

ADVOCACY CAPACITY BUILDING STAKEHOLDER MANAGEMENT TECHNOLOGY DEVELOPMENT

Information and Communication Technology for Peace

The Role of ICT in Preventing, Responding to and Recovering from Conflict

Preface by
Kofi Annan

Foreword by
Micheline Calmy-Rey

By **Daniel Stauffacher, William Drake, Paul Currion and Julia Steinberger**

United Nations

United Nations Information and Communication Technologies Task Force

ICT for peace

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."

ICT for peace foundation

ICT4Peace's interlinked Areas of Work:

1. Since 2004 using ICTs, new media etc. by the international community/UN for Peaceful Purposes inter alia humanitarian operations, peace-keeping and peace building; 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 Law, Norms, CBMs, Capacity Building = UN GGE, OSCE, ASEAN, ARF, OAS, AU)

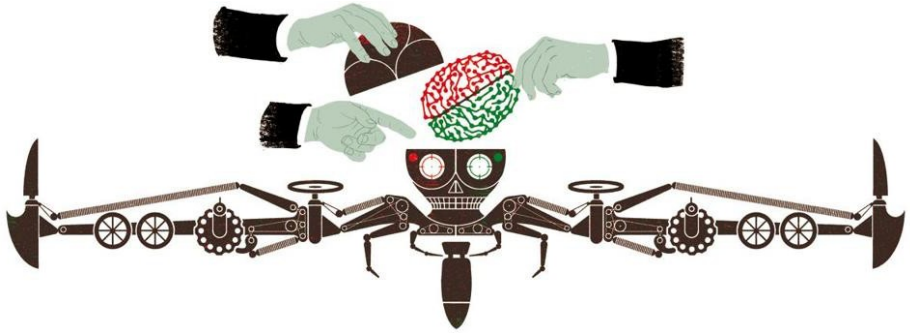
3. 2016 Mandate by UN Security Council for regarding Prevention of Use of ICTs for Terrorist Purposes (also called Tech Against Terrorism).

4. Artificial Intelligence (AI), Lethal Autonomous Weapons Sytems (LAWS) and Peace Time Threats in Cooperation with Zurich Hub for Technology (ZHET)

5. AI, Fake New and Democracy in cooperation with ZHET

Artificial Intelligence

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

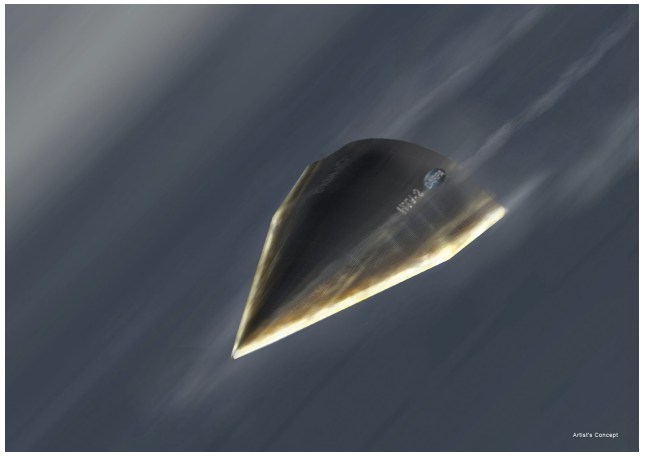


Lethal Autonomous Weapons Systems

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

United Nations Convention on Certain Conventional Weapons

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

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

Further ways of weaponizing AI + other emergnig technologies

1. LAWS during law enforcement (i.a. crowd control, hostage situations)
2. Autonomy in Cyberspace
3. Converging and merging of different technologies: e.g. AI + biotechnology

Deadly Rover, Israel. Source: Wired

Peace-Time Threats

1. AI-enabled technology (+ affective computing) and deception/propaganda
2. AI-enabled technology in the justice system
3. AI-enabled technology in light of resource-scarcity during times of crisis
4. Convergence of technologies: influence scope, and velocity -> unknown system-wide impact
5. Convergence of technologies (also biotech + biomedical data) in cyberspace: exacerbation of cybersecurity vulnerabilities

What do we need? I

We need to understand what is happening:

Current technological research, esp. AI research, allows us to create technological instruments that may lose their instrumental character because we gradually give away responsibility for the outcomes of their usage.

Do we want to limit the space of human responsibility in the world or increase it?

What do we need? II

- Holistic understanding of all (biotech, molecular nanotechnology, AI) the potential peace and security implications of new technologies, as well as the converging nature of those technologies
- Change in educational paradigms: inclusion of awareness about social impact of human creations at primary school level
- Encouraging interdisciplinary dialogue between ‘fast’ computer scientists/ software engineers and ‘slow’ philosophers and sociologists
- Setting clear goals: AI as assistance for or replacement of humans?
- Questioning the human-machine analogy and language use

What do we need? III

Political level:

- Creation of a constant national policy-technology interface through, e.g. fixed state ministers of AI/ technology
- Permanent scientific expert groups for different weapons areas/ tech sectors at UN-level

Civil society, incl. private sector and academia:

- Engaged debate on property rights on source codes of AI-enabled technology
- Increased engagement of civil society on questions of human control and responsibility for technological outcomes
- Increased and eventually constant dialogue between tech experts and civil society. Technologist must learn to transfer their knowledge in a practical way.