Summary document for UN Secretary-General's High-Level Panel on Digital Cooperation

In response to a call for written submissions for the consideration of the United Nation's High-level Panel on Digital Cooperation, the International Committee of the Red Cross (ICRC) is pleased to provide herewith some key considerations and observations related to trends in the development and deployment of digital technologies and international cooperation in the digital space. The ICRC stands willing to provide more in-depth analysis if required.

The ICRC is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavors to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. In order to implement the mandate it received from the international community,[1] the ICRC carries out its activities in full conformity with its fundamental principles of humanity, neutrality, impartiality and independence and its standard working modalities, in particular confidentiality.

In its new Institutional Strategy 2019-2022, the ICRC has placed particular emphasis on embracing digital transformation in a people-focused manner. This recognizes that the digital revolution is fundamentally transforming the way people live, work and relate to one another, including in armed conflicts and other situations of violence.

> *Digital technologies and artificial intelligence are transforming the way people and organizations function in both the physical and virtual worlds. Digitalization is also altering the way States, NSAGs and other actors interact with populations and protect or restrict fundamental rights, and also how they manage security and conduct warfare. The global digital transformation is changing the nature of humanitarian action, particularly in relation to the digital dimensions of protection, trust and privacy-related issues. While we may not be able to predict where technological progress will lead us, we know that we must equip ourselves to understand its exponentially increasing impact on our environment, so that we can exploit the opportunities it offers and mitigate the risks it carries.*[2]

The following key themes are highlighted for the UN Panel's consideration:

1. **New technologies and International Humanitarian Law**

Technological developments have given, and will continue to give, rise to new methods and means of warfare, such as cyber-attacks, armed drones and autonomous weapons systems, raising novel humanitarian and legal challenges. When developing or acquiring any new weapon, means or method of warfare, it is vitally important that a State assess whether it complies with international humanitarian law.

[1] The mandate of the ICRC is based on the Geneva Conventions of 1949, their Additional Protocols, the Statutes of the International Movement of the Red Cross and Red Crescent, and the resolutions of the International Conference of the Red Cross and Red Crescent.

[2] Extract from the ICRC's Institutional Strategy 2019-2022, p. 22

The ICRC would like to draw the Panel's attention to a number of reports published by the ICRC of relevance in this regard:

(a) As part of continuing reflections on the legal and ethical issues raised by autonomous weapons systems, the ICRC convened a round-table meeting in Geneva from 28 to 29 August 2017 to explore the ethical aspects. The report - "Ethics and autonomous weapon systems: An ethical basis for human control?" - summarizes discussions and highlights the ICRC's main conclusions. See icrc.org

(b) To coincide with the first meeting of the Group of Governmental Experts of the High Contracting Parties to the Convention on Certain Conventional Weapons on autonomous weapon systems in November 2017, the United Nations Office for Disarmament Affairs published a collection of articles: "Perspectives on Lethal Autonomous Weapon Systems". The ICRC contributed an article entitled: "Autonomous weapon systems under international humanitarian law". This article, and the other contributions, are available to download from the the UN website : Perspectives on Lethal Autonomous Weapon Systems

(c) Cyber is relevant from three perspectives:

a. the potential human cost and humanitarian consequences of cyber operations, in particular during armed conflict, and the potential risk they may affect e.g. the delivery of health, care, transportation systems, electricity and drinking water networks, dams, and chemical or nuclear plants with wide-reaching consequences; The ICRC organized and hosted an expert meeting in Geneva, Switzerland, in November 2018 on the potential human cost of cyber operations, a report from which will be published in 2019.[3]

b. applicability of international humanitarian law (IHL): for the ICRC, there is no question that IHL applies to and restricts the use of cyber capabilities as means and methods of warfare during armed conflicts, as it does for any other new technology used in conflict. Any use must respect the principles of distinction, proportionality and precautions. Notably, critical civilian infrastructure are civilian objects and therefore protected against cyber attack, unless they have become military objectives. This has been discussed in particular in the ICRC Report "International humanitarian law and the challenges of contemporary armed conflicts" (pp. 39 – 44).

[3] For more details on the issues at stake, see L. Gisel and L. Olejnik, 'The potential human cost of cyber operations: Starting the conversation', ICRC Law and Policy blog, 14 November 2018

c. digitalization of an humanitarian organizations operational response increases the risk of a cyber-attack which could impact or prevent the capacity to provide humanitarian services.

2. Data Protection and Humanitarian Action

The provision of services to vulnerable persons by organizations working in humanitarian emergencies such as armed conflicts, other situations of violence, migration, natural disasters, and epidemics requires the collection and processing of a great deal of, often highly sensitive, personal data. To deal with humanitarian emergencies, it is in many cases necessary for personal data to flow across and between the concerned countries. At the same time, as data protection and privacy laws develop at a faster pace, there is often a lack of capacity and expertise to analyse how developing data protection and privacy rules actually apply to data collected for humanitarian purposes, and about how technology functions, which is a risk factor in the humanitarian sector.

Protecting individuals' personal data is an integral part of protecting their life and dignity. This is why personal data protection is of fundamental importance for humanitarian organizations. Recent developments in new technologies have meant that the processing of ever-increasing quantities of personal data in an interconnected world has become easier and faster. This has also given rise to concerns about the possible intrusion into the private sphere of individuals and to regulatory efforts worldwide to respond to these concerns. The Handbook on Data Protection in Humanitarian Action has been published as part of the Data Protection in Humanitarian Action project, organized jointly by the ICRC and the Brussels Privacy Hub.[4] See icrc.org.

This Handbook is not intended to replace compliance with applicable legal norms, or with data protection rules, policies and procedures that a particular organization may have adopted. Rather, the handbook seeks to raise awareness and assist humanitarian organizations in ensuring that they comply with personal data protection standards when carrying out humanitarian activities, by providing specific guidance on the interpretation of data protection principles for humanitarian action, particularly when new technologies are employed.

3. Metadata

The humanitarian sector's growing use of digital and mobile technologies creates records that can be accessed and misused by third parties, potentially putting people receiving humanitarian aid at risk. A joint report from Privacy International and the International Committee of the Red Cross (ICRC) - *The humanitarian metadata problem: 'Doing no harm' in the digital era* – explains how third parties could, for example, look at the metadata of

[4] The content of the handbook was developed in a series of workshops held in Brussels and Geneva in 2015–2016, with representatives from humanitarian organizations (including humanitarian practitioners), data protection authorities, academics, non-governmental organizations, researchers and other experts. They came together to address questions of common concern in the application of data protection in humanitarian action, particularly with respect to new technologies.

someone's mobile telephone messages to infer details like sleep patterns, travel routines or frequent contacts. That kind of information could pose risks to a person in an armed conflict environment. The report details what metadata is collected or generated when humanitarian organizations use telecommunications, messaging apps or social media in their work. While the report doesn't advocate for privacy or against surveillance, it demonstrates how ensuing surveillance risks could obstruct or threaten the neutral, impartial and independent nature of humanitarian action. To remedy this, the report recommends a more systematic mapping of who has access to what information in order to anticipate how individuals might be profiled or discriminated against. It also encourages humanitarian organisations to improve digital literacy among their staff, volunteers – and most importantly, the people they serve.

4. Digital risks in situations of armed conflict

The introduction of increasingly sophisticated digital tools, software, platforms and broader internet access etc. have facilitated and improved the delivery of many humanitarian processes and services to affected populations. Although access remains uneven both at the macro and micro level, populations are also increasingly resorting to digital technologies to communicate and share or search for information. Finally, for many people, digital technologies are playing a key role in accelerating development, reducing poverty, improving accountability and democracy in developing countries including those affected by social, economic and political instability and/or conflict.

While digital technologies can offer many opportunities to improve the lives of individuals and communities affected by situations of armed conflict or violence, there is also growing concern around their possible negative implications both in terms of risks and harms for already vulnerable populations. However, there is still little shared clarity on the scope and nature of those risks as well as the humanitarian consequences for populations. The ICRC, working with experts from within the humanitarian sector, tech companies and academics, held a two-day symposium focusing on the digital risks for populations in armed conflict, how they manifest themselves and what consequences these have for affected populations and those organizations who try to serve them. A report of the event will be published in early 2019.

The three main scenarios discussed on the first day were: (a) Surveillance, monitoring and intrusion ; (b) The weaponisation of information ; (c) Cyber operations.

How data is collected, aggregated, accessed, analysed, spread and even manipulated is affecting the risks to individuals who would not see themselves as part of a conflict or battlefield. The use of technologies to bring efficiency and scale are being deployed with the very real risk that the necessary due diligence has not been carried out. Due diligence is necessary to assess the potential impact on privacy, immutability, security of systems, and the identification of risks in order to be able to take appropriate action. It is important to assess the technical, legal and operational requirements necessary in order to safely leverage emerging technologies in humanitarian programming.

It is important to advocate for an humanitarian purpose driven use of data collected for humanitarian responses, i.e. to collect data respecting the needs of beneficiaries, data minimization even where technologies allow so much more data to be collected than is necessary for effective programming, as well as to recognize the need for policies and consent related to how data is used, etc. This is a complex endeavour and requires the relevant investments in understanding the vulnerabilities and needs of people affected by armed conflict, the risks that people are exposed to, and specific characteristics and capabilities of technologies that may actually cause more harm than good when applied in situations of conflict.

As conventional ways of conducting armed conflict are being enhanced, transformed, or replaced by digitally-derived forms of violence, persecution and exploitation, affected populations are being exposed to new vulnerabilities. People might have to contend with cyber-attacks that affect life-saving critical infrastructure and communications systems. They will also have to navigate with emergent and subtle forms of digital surveillance, electronic exploitation, and the "weaponization" of information. A dialogue across sectors is needed.

5. Misinformation and misuse of social media platforms

In recent years, there has been a multiplication of situations in which hate speech on social media platforms has exacerbated violence among communities. In a highly politicized, polarized or/and weaponized environment, misinformation and propagation of content that can spread violence can have lethal consequences. Focusing on content alone is not enough, it is important to focus on ensuring that mechanisms are in place to avoid that there is an encouragement and amplification of discussions in ways that can be harmful. There is a knowledge gap between the technology and humanitarian sectors and even more, those who are working in organizations, especially amongst populations that may have little knowledge about how technology functions for or against them. In contexts with a *low level of digital literacy*, populations tend to believe what is featured on social media platforms. It is thus important to raise levels of digital literacy in order to support increased resilience and protection. However, it is also important to guard against generic digital literacy models and training. For such programmes to be effective, a risk assessment needs to be carried out with the affected populations in order to understand their needs and digital behaviours: how they use their devise and the technologies they contain, and for what purpose. Thus, digital literacy programme should ideally be grounded on an evidence-based need and risk assessment. At this stage there no standard protocol or guidance as to how to carry out such types of assessment that could inform an appropriate response.

6. Artificial Intelligence and Humanitarian Action

The so-called Digital Revolution is transforming the humanitarian sector. It is introducing innovative ways of capturing and exploiting digitalized information alongside new forms of digital humanitarian assistance. Many organizations are implementing pilots focusing on areas such as, biometrics as a form of identifying people, drones as a way to bring assistance to remote places, block chain as a way to safeguard information.

While digital technologies can offer many opportunities to improve the lives of populations affected by armed conflict, there is also growing concern around their possible negative

implications. This include the (often unintended) side-effects of digital data experimentation, violations of privacy, and mishandling of sensitive information that goes along with the humanitarian sector's efforts to deploy emerging technologies in already fragile contexts

In the field of AI, there are already see some key issues emerging which can facilitate such a debate.

a. Data Aggregation: AI generates the opportunity to read the environment better and better understand the challenges of humanitarian action, with the purpose of better responding. But it also aggregates "too much information", which can become a risk for certain people (i.e. if a party to conflict leverages AI to specifically target certain minorities or armed groups). We know that in highly complex environments the same technology/data can be used negatively. It is important to identify how do you protect people in these environments.
b. Biases: We have seen the limitations of AI e.g. in facial recognition where systems have been trained (the machine has learned to recognize) on data sets that are predominantly biased towards certain characteristic e.g. "white and male". Such distortions or biases inherent in the training of systems have to be corrected to enable their use, this is not simple. We need to work closely with the Tech sector to recognize the biases and identify how vulnerabilities can be addressed.

These issues are not just technology related. It is important to understand how to maintain trust in the digital age, and ensure that we keep humanitarian purpose and the people humanitarian organizations are there to assist and protect firmly at the centre of any developments in order to ensure the humanitarian response capacities do no harm in their application.

To best enable humanitarian organizations to meet such challenges, it is important to ensure that we:

a. **understand the risks, protection issues, ethical concerns and challenges before building digital solutions**: Rather than focusing too much on the opportunities and zooming too quickly into the technical level, first we need to collectively understand the potential impacts on vulnerable populations, and design the broader elements of the use of AI;

We should also be reviewing ideas against the criterion of having a **valid and important humanitarian purpose for developing a certain digital capability or using certain data.**

Geneva, Switzerland. January 2019