Symposium on Cybersecurity & Data Protection in Humanitarian Action

23 – 25 January, 2024

Luxembourg

DigitHarium

Luxembourg Aid and Development: The Ministry of Foreign and European Affairs, Defense, Cooperation and Foreign Trade Directorate for Development Cooperation and Humanitarian Affairs is responsible for Luxembourg's development cooperation and humanitarian action policy. Its mandate includes implementing Luxembourg's general development cooperation strategy (The Road to 2030) in close collaboration with its public and private partners as well as international and multilateral organizations in line with the principle of "leaving no one behind".

Luxembourg Red Cross: The Luxembourg Red Cross, a member of the International Red Cross and Red Crescent Movement, stands in solidarity with the most vulnerable around the world. Their teams of the "aide international" unit can deploy emergency support to those affected by conflict as well as natural and man-made disasters.

Luxembourg's National Data Protection Commission: Commission Nationale pour la Protection des Données (CNPD) is an independent public authority created in 2002 and organized by the Act of 1 August 2018 on the organization of the National Data Protection Commission and the general data protection framework. Its mission is here to supervise the lawfulness of processing activities, covering the collection, use and transfers of data relating to identifiable individuals. It also protects the freedoms and fundamental rights of natural persons, in particular their right to privacy.

The Interdisciplinary Centre for Security, Reliability and trust (SnT) at the University of Luxembourg: SnT conducts internationally competitive research in information and communications technology (ICT) with a focus on creating socio-economic impact.

Luxembourg House of Cybersecurity (LHC): The Luxembourg House of Cybersecurity is the gateway to cyber resilience in Luxembourg and aims at capitalising on and further developing innovation, collaboration and capacity building. As a central player, the LHC is home to all types of cybersecurity-related activities and together with its two hosted centres CIRCL (Computer Incident Response Center Luxembourg) and NC3 (National Cybersecurity Competence Center) as well as its identified partners, supports, fosters and serves the Luxembourg economy and society.

International Committee of the Red Cross (ICRC): Established in 1863, the ICRC operates worldwide, helping people affected by conflict and armed violence and promoting the laws that protect victims of war. As an independent and neutral organization, its mandate stems essentially from the Geneva Conventions of 1949. It is based in Geneva, Switzerland and employ over 21,000 people in more than 100 countries.

DigitHarium: the DigitHarium is a global forum to discuss and debate digital transformation within the humanitarian sector, with a focus on humanitarian protection, policy, ethics and action. Part of the Humanitarian Data and Trust Initiative, the DigitHarium provides a space where humanitarian, diplomatic, academic and technology practitioners can meet to collaborate in order to find local and global solutions to today's digital dilemmas.

Introduction

The rise of new digital technologies has transformed humanitarian action. Incorporating digital tools into humanitarian work has led to an increase in efficiency and a reduction in costs — by facilitating faster economic assistance and greater autonomy through digital cash transfers, for example, or by allowing lifesaving information to be communicated to a broader, hard-to-reach public via social media. However, these digital tools also generate novel risks affecting both people living through crises and the organizations that aim to support them. These risks can arise through the increase in surveillance that technology often engenders, the pervasiveness of misinformation, disinformation and hate speech with potentially lethal real-life consequences, and the possibility of exclusion due to digital divides. In other words, they can erode the dignity, integrity, and security of the affected populations. In parallel to this digital transformation of humanitarian dynamics, the tech industry is increasingly present in humanitarian contexts as service providers for both affected populations and humanitarian organizations. In this fast-evolving space, new technology areas and technological actors continue to emerge and manifest their relevance for humanitarian action, and the implications of deploying them are often difficult to understand, let alone anticipate.

Tackling these challenges is essential to ensure that humanitarian action can remain meaningful and effective for the communities affected by humanitarian emergencies. It is also key to enable humanitarian organizations to leverage technologies responsibly while upholding the principle of “do no harm”, keeping affected people at the center and upholding their dignity when processing their data, and remaining accountable to them for their use. Participants from each field – whether they be from humanitarian organizations, regulators, civil society, academia, or private companies – have a unique stake in the issues at hand. For instance, humanitarian organizations must consider the realities of the field alongside budgetary restraints and their responsibility to donors. Likewise, policymakers, civil society, and academics each come to the table equipped with their own experiences, insights, and challenges. Indeed, actors in the private sector have also grappled with these issues, as made evident by numerous public-private technology-centric partnerships that have emerged over recent years. Given this wealth and diversity of experience, participants of the Symposium are well placed to put forward viable ideas and solutions.

This second edition of the Symposium of Cybersecurity and Data Protection in Humanitarian Action builds on the insights from the first edition, as well as to bring together the experience, expertise, and ideas of key stakeholders from the public, private and humanitarian sector, as well as civil society and academia, to identify – and, if possible, anticipate – challenges and areas of concern in the use of technology in humanitarian action, and to find, together, possible ways to navigate them.

Day 1 → Tuesday 23 January 2024

Rooms	08:00 - 09:00	09:00 - 9:45	9:45 - 10:00	10:00 - 12:00
Entrance and Hall	Registration and breakfast			
Conference Room		Cyber Range opening session	Move to Cyber Range rooms	
Salle FR				Cyber Range
Salle UK				Cyber Range
Salle PL				Cyber Range
Salle IT				Cyber Range
Salle BE				Cyber Range
Salle CZ				Cyber Range
Salle HU				Cyber Range
Salle GR				Cyber Range

Day 2 → Wednesday 24 January 2024

Rooms	08:00 - 09:00	09:00 - 10:15	10:15 - 10:30	10:30 - 11:15	11:15 - 11:45
Entrance and Hall	Registration and breakfast				
Conference Room		Opening plenary session			
Salle DE				Mapping digital risks and digital harms	
Salle FR				Humanitarian health services and digital tools	
Salle UK				Neutrality, impartiality, and independence at the network layer	Coffee break
Salle PL				Civilianization of conflict through cyber means	
Salle IT				Neutrality, impartiality and independence in software tools: Free and open-source software in humanitarian action	
Salle BE					
Salle SE				Hackathon	
Salle PT				Hackathon	

Move to Working Sessions rooms

Day 3 → Thursday 25 January 2024

Rooms	8:00 - 09:00	09:00 - 09:15	09:15 - 10:30	10:30 - 11:00
Entrance and Hall	Breakfast			
Conference Room				
Salle DE			Navigating trust and safety as tech companies in armed conflict	
Salle FR			Marking protected objects in a digital space: Digitalizing the red cross and red crescent and red crystal emblems?	Coffee break
Salle UK			The principle of humanity and humanitarian uses for artificial intelligence	
Salle PL			Open-source information and personal data protection	
Salle IT			Measuring the harm of cyber operations to the people affected	
Salle SE			Hackathon	
Salle PT			Hackathon	

Move to Working Sessions rooms

Public sessions accessible to all participants

12:00 - 13:30	13:30 - 15:00	15:00 - 15:30	15:30 - 17:00	17:00 - 17:30	17:30 - 18:00	18:00 - 19:30
					Digital Dilemmas presentation	Aperitif (at Novotel)
				Cyber Range closing session		
Lunch break	Cyber Range	Coffee break	Cyber Range			
	Cyber Range		Cyber Range			
	Cyber Range		Cyber Range			
	Cyber Range		Cyber Range			
	Cyber Range		Cyber Range			
	Cyber Range		Cyber Range			
	Cyber Range		Cyber Range			
	Cyber Range		Cyber Range			

11:45 - 12:45	12:45 - 14:15	14:15 - 15:15	15:15 - 15:45	15:45 - 16:45	16:45 - 18:30
					Aperitif (at ECCL)
		Understanding the digital risks and opportunities for children affected by armed conflict, including personal data protection			
		Safeguarding humanitarian connectivity: The issue of dual-use satellites			
	Lunch break	Data protection by design and biometrics in humanitarian action	Coffee break		
		Data protection, digital risks, data responsibility and ethics: How these frameworks for analysis interact to guide responsible use of technology in humanitarian action			
		Neutrality, impartiality and independence and the cloud: Achieving exclusively humanitarian use of humanitarian data			
		Using open-source information analysis to document digital harm			
		Hackathon		Hackathon	
		Hackathon		Hackathon	

11:00 - 12:15	12:15 - 13:45	13:45 - 14:15	14:15 - 15:15	15:15 - 15:45	15:45 - 16:45	16:45 - 17:45
		Keynote address	1st Panel		2nd Panel	3rd Panel
	Lunch break			Coffee break		
			Hackathon		Hackathon wrap up	
			Hackathon		Hackathon wrap up	

Symposium Composition

The Symposium on Cybersecurity and Data Protection unfolds over the course of three days and is composed by different activities and elements.

Cyber Range

The Symposium will unfold over the course of three days. The first day will be dedicated to the humanitarian Cyber Range, a group-based exercise that makes the participants respond to various cyber threats as a humanitarian organization, through a series of strategic and technical tasks.

Working Sessions

The second and third day of the Symposium will be dedicated to two parallel initiatives. A series of multi-stakeholder closed-door discussions, which will take place under the Chatham House rule. Each participant will be assigned a "path" -- a set of three working sessions, each of which has complementary thematic content and is relevant to the skillset of the attendees.

Digital Dilemmas Exhibition

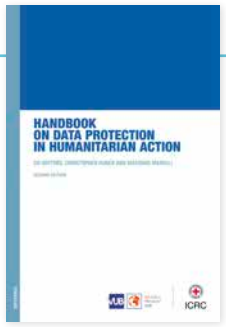
On display for all Symposium's participants, the Digital Dilemmas Exhibition will offer an immersive experience that reflects upon the impact of digital technologies on civilians in conflict.

Hackathon

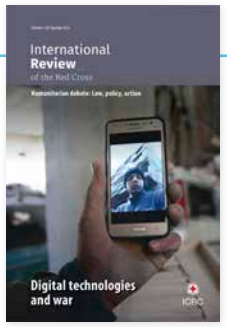
Simultaneously, the co-organizers will also be hosting a hackathon which will gather technical specialists around specific challenges. While the working sessions will discuss and advance the reflections on key humanitarian issues, the hackathon brings together developers and practitioners to create and co-create technical, legal and policy tools, which are necessary to launch the digital humanitarian open-source community.

Publication highlights

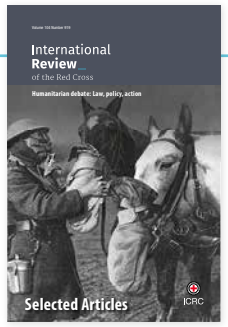
The Symposium will also host a library, in which several relevant publications from our co-organizers, participants, and other relevant experts will be on display. These publications include:



→ The Handbook on Data Protection in Humanitarian Action



→ The International Review of the Red Cross - IRRC No. 913 Digital Technologies and War

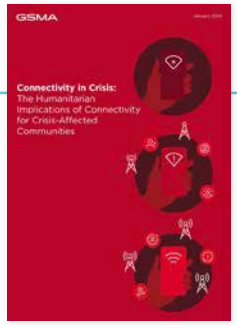


→ The International Review of the Red Cross - IRRC No. 919 Selected Articles

→ Protecting Civilians Against Digital Threats During Armed Conflict

→ The Value of Open Source in The Open Data Community

→ LHC Forum Report #2 on Post Quantum Security



→ Connectivity in crisis: the humanitarian implications of connectivity for crisis affected communities

→ Vos données ? Vos droits ! Protection des données : vos droits et comment les faire valoir

Working Sessions

Neutrality, impartiality and independence in software tools: Free and open-source software in humanitarian action

→ Wednesday 24 January
Ⓘ 10:30 - 12:45
Salle IT

Humanitarian organizations increasingly rely on digital tools, not only to communicate and to coordinate their daily activities but also to offer digital services directly to affected communities. They depend on a range of software products often developed and commercialized by tech companies. This growing dependence can make them vulnerable to trends – politicizing and polarizing – in cyberspace. These trends include allegations and perceptions of participation – intentional or unintentional – in implementing national security priorities and surveillance; business models based on data exploitation or profiling; explicit support for some parties to conflict and/or boycotting of others; and participation in global competition over digital infrastructure and standard setting.

This session starts from the assumption that these geopolitical tensions that have infiltrated the tech sector may – if they are not already doing so – affect humanitarian organizations that use the tools provided by tech companies. More specifically, by using such tools to manage their growing digital footprint, humanitarian organizations may be endangering the perception – and the acceptance based on that perception – that they are neutral, impartial, and independent organizations capable of acting on exclusively humanitarian grounds. This session therefore looks at free and open-source software (FOSS) tools as possible alternatives to address the issues identified above.

The objective of this session is to examine these challenges and gather insights and recommendations for developing a pragmatic FOSS strategy for humanitarian organizations.

Neutrality, impartiality and independence and the cloud: Achieving exclusively humanitarian use of humanitarian data

→ Wednesday 24 January
Ⓘ 14:15 - 16:45
Salle IT

As humanitarian organizations' use of digital technology grows, so too does the amount and variety of the data they have to handle. Some of this data, crucial for fulfilling their mandate, can be of great sensitivity. And their sources are multifarious: internal information, correspondence with states and other actors, and confidential personal information on members of affected populations.

Data collection in humanitarian settings, for organizations carrying out neutral, impartial and independent humanitarian action, requires a steadfast commitment to affected communities that their data will be used only for humanitarian purposes. In conflict environments, it also requires pledging to parties to armed conflict or other situations of violence that the data collected will be used in a neutral, impartial and independent manner, and for exclusively humanitarian purposes.

The use of cloud-based tools involves third-party tech companies, which then become in effect intermediaries for humanitarian action. These companies have no humanitarian mandate and do not enjoy the privileges and immunities that would enable them to fulfil such a mandate in a neutral, impartial, and independent manner. They are also vulnerable to the exercise of jurisdictional authority by the countries in which they operate, and cannot guarantee that data will not be accessed by governments for purposes that are not exclusively humanitarian. This is an important consideration, because a number of different actors have an interest in gaining access to humanitarian data for reasons unrelated to humanitarian action – for instance, to gain a strategic and operational advantage over adversaries.

Challenges related to ensuring exclusive jurisdictional authority over data are also of concern to states, in connection with data related to their functions and their citizens. Initiatives are therefore being proposed at state and regional levels to regulate the technology and services used in a digital infrastructure: these initiatives often refer to the notion of "digital sovereignty".

This session will focus on what international humanitarian organizations can do – when employing the services of third-party providers – to ensure that data under their control are used for exclusively humanitarian purposes. At this session, technical solutions – like "trusted execution environments" and homomorphic encryption – will be examined, as will organizational measures and legal measures such as ensuring the reliability of contractual clauses and the precise wording of the privileges and immunities of international organizations. The session will seek to develop a framework for humanitarian organizations to assess, analyse and manage risks, together with a toolkit for risk mitigation measures along the lines suggested above.

Navigating trust and safety as tech companies in armed conflict

→ **Thursday 25 January**
09:15 - 12:15
Salle DE

This session is designed to discuss the steps that tech companies can take to ensure that conflict-affected people are safe and effectively protected when using specific digital technologies. During armed conflict, tech companies provide services and also act as intermediaries for humanitarian services. Their actions can have a profound effect on people's lives. Loss of essential services due to cyber operations; harm caused by collection and exploitation of data – including by third parties – for both surveillance and commercial purposes or for monetization of data; and harmful information spreading on social media and beyond, and lack of trustworthy information: these are some of the most significant risks posed by technology to people affected during a crisis. Decisions made by companies – related to product design, for instance – can improve safety or exacerbate vulnerability during conflict; such decisions must be taken in full knowledge of their potential for harm in armed conflict. This working session will seek to identify practicable measures to ensure that the digital products and services used by people caught in situations of armed conflict are as safe, easy and intuitive to use as possible. It will also seek to identify means to ensure that intermediation of humanitarian action through commercial service providers does not risk eroding the trust of affected people in the neutrality, impartiality and independence of humanitarian action. The working group will discuss how to continue to grow a global community of experts who are interested in armed conflict, digital technology, and corporate behaviour; willing to help design and implement better and more coherent policies and self-regulatory decision-making; and willing also to advocate in this regard.

Civilianization of conflict through cyber means

→ **Wednesday 24 January**
10:30 - 12:45
Salle PL

A number of recent developments suggest that civilian involvement on the digital battlefield is growing, from their engagement in offensive cyber operations against enemy targets to the repurposing of civilian smartphone apps for military use. It is now easier than ever to involve civilians in military cyber operations and to harm them with the same means – and to do so simultaneously, given the conduct of certain parties to conflict. This has blurred the distinction between civilians and combatants, and put civilians at great risk of harm during armed conflict. This session will explore the risks to civilians involved in military cyber operations, and will seek to understand the legal constraints that might be applicable to such forms of civilian involvement on the digital battlefield. The session will also look further into the implications – for international humanitarian law and the conduct of warfare – of these new technologies, and the ethical issues arising from them. It will also look into ways of tackling these difficulties.

Using open-source information analysis to document digital harm

→ Wednesday 24 January
🕓 14:15 - 16:45
📍 Salle BE

The role and importance of digital open-source information (OSI) has grown with the rise in the digitalization of conflict. Content posted on social media is used by a variety of actors to provide evidence of potential war crimes and to support accountability processes. It is also a crucial source of information for civilians affected by armed conflict. However, as humanitarian organizations have begun to recognize, these digital technologies, besides their potential to play a positive and even life-saving role in armed conflict, can also endanger the lives, dignity and resilience of civilians in many different ways.

This working session will identify the tools necessary to document and understand such risks, and will explore possibilities for the use of OSI analysis by humanitarian organizations to detect, measure and mitigate digital harm. It will also assess the challenges to applying these tools in humanitarian action, and in accordance with working modalities linked to confidentiality, which require protection dialogue to be carried out primarily via confidential bilateral engagement rather than publicly. The tensions between the working modalities of humanitarian organizations and the humanitarian functions of OSI will be discussed at this session, to enable participants to think through responsible ways of using this important resource.

Open-source information and personal data protection

→ Thursday 25 January
🕓 09:15 - 12:15
📍 Salle PL

The importance of adhering to applicable personal data protection frameworks is often mentioned in public guidance for processing open-source information (OSI), but seldom accompanied by examples or explained in any detail. As humanitarian organizations begin to put OSI analysis to various uses, often updating data-management processes or implementing new processes to do so, it is becoming increasingly necessary to develop a uniform approach to protecting personal data that is collected as OSI or inferred from OSI techniques. This session will proceed on the assumption that a given humanitarian organization has a legal basis to process the OSI it collects. Discussion will then focus on purpose limitation and on data subjects' rights to information and access, and their rights to objection, rectification and deletion. The aim of the session is to provide concrete guidance for the responsible use of OSI for humanitarian purposes.

Neutrality, impartiality, and independence at the network layer

→ Wednesday 24 January
🕓 10:30 - 12:45
📍 Salle UK

Humanitarian organizations have become more reliant on digital technologies as their use of digital means increases, and as digitalization becomes more pervasive among actors around them. One consequence of this is that they are increasingly affected by the dynamics of their digital infrastructure, which include global trends such as splinternets; surveillance; cyber attacks; denial or restriction of connectivity; and data-flow bottlenecks. This session focuses on the ways in which humanitarian action is affected by the dynamics of the digital infrastructure, particularly the network and routing elements, on which it relies. The session seeks to develop understanding of the threats to humanitarian organizations' ability to safeguard the neutrality, impartiality, independence and security of their routing of data flows.

The session pays particularly close attention to international humanitarian organizations, which enjoy privileges and immunities that enable them to fulfil their humanitarian mandate – in full respect of their neutrality, impartiality and independence – and safeguard the exclusively humanitarian nature of their work. These humanitarian organizations may need to determine how to route their data flows in a way that ensures respect, at all times, for the legal inviolability of their data. This session also aims to discuss concrete means of addressing these challenges. This may include technical solutions available within current internet infrastructure (e.g. peering) and alternatives to this

infrastructure that can ensure a reliable, stable and resilient infrastructure and that incorporate deliberate routing protocols (e.g. Scalability, Control and Isolation on Next-Generation Networks, or SCION). It may also include policy solutions, such as recommendations for states and humanitarian organizations, particularly those having the status of "international organization".

Safeguarding humanitarian connectivity: The issue of dual-use satellites

→ **Wednesday 24 January**
14:15 - 16:45
Salle FR

Humanitarian organizations are at work around the world, and often in crisis settings or remote areas where infrastructure and connectivity may be inadequate. Satellite systems can support their response to humanitarian crises and also assist in their day-to-day activities. They are valuable for both humanitarian organizations and the people affected by crises. However, humanitarian organizations are not alone in making use of satellite systems; governmental and military entities do so as well.

Many different actors use satellite systems and depend on them for military and other purposes. This has created a fresh set of challenges for humanitarian organizations. The infrastructure is managed mainly by private companies. States are becoming more and more dependent on the private sector for satellite connectivity – particularly on Low/Medium Earth Orbit satellites; and the strategic importance of these satellites is growing by the day. This dependence is attributable mainly to states' wish to amortize the costs of setting up and operating the infrastructure. The result is dual use of these satellite systems, a situation in which the same infrastructure and potentially the same communication frequencies are used for government and military purposes on the one hand and civilian and humanitarian purposes on the other.

This session will first consider the issues that humanitarian organizations might have to confront because of such dual use. For example, the session will explore how dual use of the same tools – for military use by one party to a conflict against another, and by humanitarian organizations for humanitarian purposes in connection with the same conflict – might call into question the neutrality, impartiality and independence of the humanitarian organizations concerned.

The session will also seek to clarify whether dual use of the assets and frequencies in question might impair the ability of parties to armed conflict to distinguish between civilian objects – specifically humanitarian infrastructure – and military objects, and whether this might create new risks for humanitarian organizations and civilian infrastructure.

This session will then explore possibilities for addressing these concerns and technical and legal solutions – and policies – such as segregating infrastructure logically and physically or simply marking them as protected objects, and setting standards, drafting regulations or protecting a "humanitarian frequency" for satellite communication.

Marking protected objects in a digital space: Digitalizing the red cross and red crescent and red crystal emblems?

→ **Thursday 25 January**
09:15 - 12:15
Salle FR

Cyber operations are becoming a reality of armed conflict. A growing number of states are developing military cyber capabilities, and their use in armed conflict is likely to increase. The ICRC has issued public warnings about the potential human cost of cyber operations, and in particular, about the vulnerability of the medical sector and humanitarian organizations to harmful cyber operations, both having been targeted in recent years.

With all this in mind, the ICRC decided to investigate the possibility of incorporating the red cross, red crescent and red crystal emblems in information and communication technology, for instance by means of a "digital emblem". The ICRC has – since 2020 and in partnership with a number of research institutions – been exploring the technological feasibility of developing a digital emblem. It convened a group of international experts to assess the potential risks and benefits associated with such an emblem. At the same

time, the ICRC – with the support of the Australian Red Cross – has consulted different National Red Cross and Red Crescent Societies about this initiative.

The idea of a digital emblem and its objectives are straightforward: for over 160 years, the distinctive emblems have been used to convey a simple message: in times of armed conflict, those who wear them, or facilities and objects marked with them, must be protected against harm. Other initiatives for identifying objects to be protected have gained ground in recent years; and proposals for the use of new technologies to expand the capabilities of the physical emblem have been suggested by various researchers. In this session, these different proposals will be discussed, to draw attention to potential shortcomings and possibilities for further improvement, and to suggest means of adoption and implementation.

Mapping digital risks and digital harm

→ **Wednesday 24 January**
10:30 - 12:45
Salle DE

The use of digital technologies in armed conflict and other violence is a growing source of offline and online harm to affected people. Humanitarian organizations continue to advance their understanding of digital risks and their harmful consequences, but further work is needed to catalogue, contextualize, and document these risks. In fact, given their digital dimension, several factors unique to cyberspace must be taken into account to understand, and subsequently catalogue and document these risks. This is essential for developing meaningful risk awareness; understanding how different stakeholders make use of digital technologies and are affected by them; and devising effective responses to the needs of affected populations.

This session therefore aims to discuss and collaboratively identify and map the various digital risks, based on the related humanitarian concerns. After doing that, the need for a detailed categorization of these risks will become clearer. In this connection, the session will also examine the difficulties associated with cataloguing and documenting these risks, and gather suggestions and recommendations for developing a detailed map of digital risks and digital harm.

Data protection, digital risks, data responsibility and ethics: How these frameworks for analysis interact to guide responsible use of technology in humanitarian action

→ **Wednesday 24 January**
14:15 - 16:45
Salle PL

Several frameworks for analysis have been suggested in connection with the new challenges created by digital transformation in humanitarian action. They include personal data protection; mapping and framing digital risks and digital harm; data responsibility; and ethics. These are often described as being alternatives to or mutually exclusive from one another. However, a closer examination of the matter can reveal how they interact and how, when used together, can guide responsible use of technology in humanitarian action. This session therefore aims to discuss how these frameworks interact and overlap, and whether it is possible for them to complement one another. Discussing the commonalities will illustrate their respective necessity, as each one of them addresses at a different level the challenges brought by the digital transformation in humanitarian action. The session will also explore how, taken together, these frameworks for analysis can have a positive impact on the humanitarian sector's approach to tackling digital harm.

Measuring the harm done by cyber operations to the people affected

→ **Thursday 25 January**
09:15 - 12:15
Salle IT

Because of the growing use of cyber operations and digital tools during armed conflict and other violence, the people affected are becoming more and more vulnerable to digital risks and to their harmful consequences. It is particularly important in this context to keep in mind a central tenet of the protection of civilians, and of the normative framework put in place to this end: the provision that military force should be proportionate, not excessive, and not indiscriminate. In order to ensure that the parties concerned can fulfil this obligation, it is absolutely essential to determine and classify the ways in which cyber operations harm the people affected.

Efforts to understand the financial costs of cyber operations have been in progress for some time, but less attention has been given to measuring the digital harm done to people affected by humanitarian emergencies. There is no shared definition of "cyber harm", and there is also no common methodology or framework available to assess and measure this harm. As a result, it may be very difficult to assess the harm done to the people affected, and thus to assess whether the harm caused is lawful in light of the normative framework, and to determine what mitigatory and protection programmes to carry out in response. Developing a concrete set of indicators of harm, and tools and standards, to measure cyber harm can contribute to strengthening the capacity to address the protection concerns of victims of these operations. In addition, a harm assessment can potentially help to increase cyber resilience, because understanding the direct and indirect harm caused by cyber incidents will help individuals and organizations to identify potential risks and vulnerabilities; prioritize anticipatory and preventive action, and responses; and develop effective mitigatory strategies to minimize harm.

The objective of this session is to examine cyber harm, develop a common understanding of it and recommend a set of indicators to measure how cyber operations can adversely affect people during armed conflicts and other violence.

Understanding the digital risks and opportunities for children affected by armed conflict, including personal data protection

→ **Wednesday 24 January**
14:15 - 16:45
Salle DE

This session examines the process of protecting children and handling their data in a manner that is responsive to their specific needs – and respectful of their rights and dignity – within the context of the proliferation of technology. It will consider closely the potential for digitalization to endanger children – in areas affected by armed conflict and other violence – in specific ways and do them particular kinds of harm; and will seek to identify means of overcoming the many challenges associated with protecting children in these complex environments. Children's use of the internet, child trafficking and the dissemination of child sexual abuse material (also known as CSAM): all this has caused alarm throughout the world; but less attention has been paid thus far to the manifestation of these risks for children affected by armed conflict. This session will pay particular attention to humanitarian crises, child-specific risks, and the principles and requirements of personal data protection for children affected by conflict and other violence.

Humanitarian health services and digital tools

→ **Wednesday 24 January**
10:30 - 12:45
Salle FR

Some of the world's most vulnerable populations – such as refugees, internally displaced persons and other people on the move – receive medical services exclusively from humanitarian organizations. Médecins Sans Frontières and the ICRC have worked towards developing effective, often digital, means of delivering such care. This session considers the risks – related to the management and protection of health data – that arise when affected people, such as migrants and refugees, rely on digital tools for health services. Health data, such as the data contained in digital medical records, are very sensitive, and their processing is subject to the most stringent data protection standards. This session asks stakeholders to discuss how the development of digitalized health services is affected by data protection standards, and asks them also to explore possibilities for ensuring that health innovation takes place in a manner that is respectful of the rights and dignity of affected persons and in line with the requirements of "Data Protection by Design".

Data protection by design and biometrics in humanitarian action

→ **Wednesday 24 January**
14:15 - 16:45
Salle UK

The use of biometrics, or "automated recognition of individuals based on their behavioral and biological characteristics", is a major development in the way humanitarian organizations incorporate digital tools in their services. Humanitarian

organizations, throughout the world, have been making increasing use of biometrics-based identification systems to manage lists of affected people and the distribution of aid. Biometrics-based identification systems offer the possibility of increased efficiency (in terms of speed, scalability, and cost-effectiveness), and reduction in fraud or misuse, in the distribution of humanitarian aid. However, relying on these tools may create significant data protection risks, because biometric data processing can lead to 'function creep', due, for instance, to pressure to reuse this data for non-humanitarian purposes; concerns over surveillance; and trust and ethical concerns arising, for instance, from false matches and difficulties related to accuracy in certain communities. This session will explore practical measures to limit these risks, by employing a "Data Protection by Design" approach. Its goals are these: create a list of such measures; explore possibilities for mechanisms that can assess the proportionality of using biometrics as a means of identification; and discuss what happens after biometrics is put into practice. The session will also examine the technical means that can be included in the design of solutions to enforce purpose limitation, which is a principle of data protection that requires that personal data be collected only for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.

The principle of humanity and humanitarian uses for artificial intelligence

→ **Thursday 25 January**
09:15 - 12:15
Salle UK

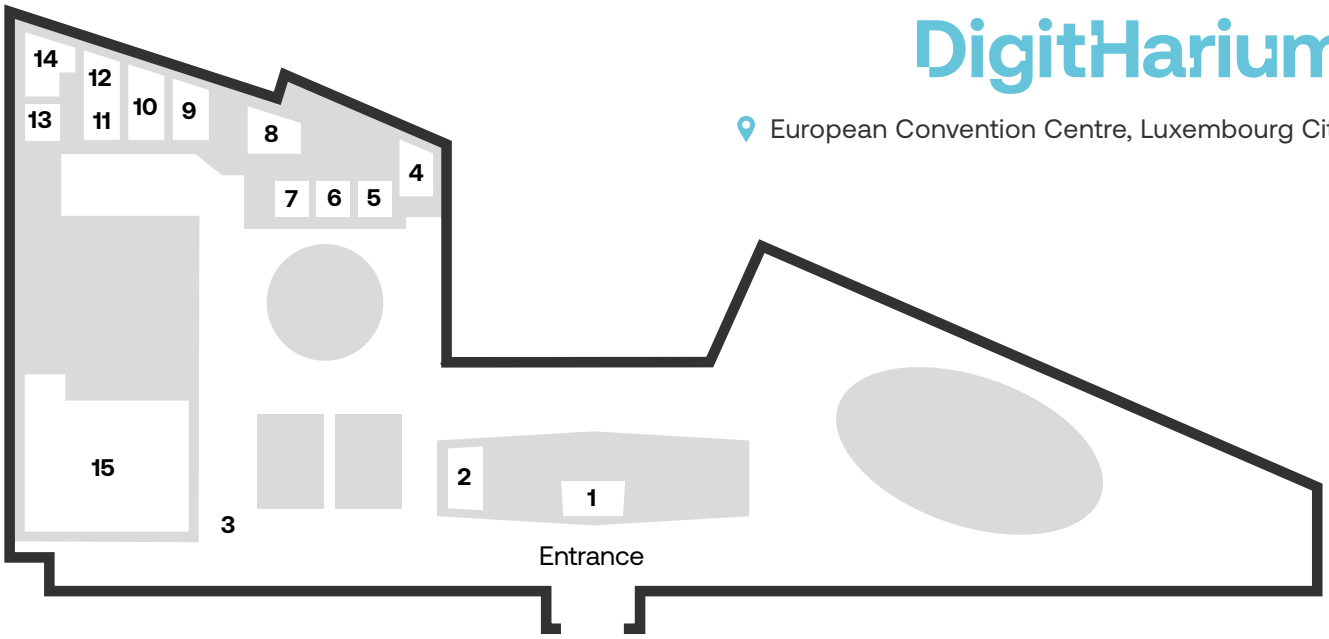
New applications using artificial intelligence (AI) are being developed every day, including in the humanitarian sector; and new tools designed to support decision-making in humanitarian action proliferate. Some of these applications provide solutions for information management, predictive analytics, environment scanning, and needs assessment. As the humanitarian sector adapts to the changes, risks, and opportunities created by developments in AI, how can humanitarian organizations ensure that digital automation does not jeopardize the human element that drives humanitarian action, and that the principle of humanity remains respected and central? The prioritization of humanity in the humanitarian application of AI must also take into account the human and environmental costs of keeping AI systems up and running. As AI tools continue to reshape emergency response planning, the response to environmental degradation, and the labour market, how can humanitarian organizations ensure the safety of human beings and respect for their dignity and agency?

This session will address all these questions and formulate recommendations for the humanitarian sector to meet these challenges. It will also make recommendations for the responsible use of AI-supported tools within the context of humanitarian action. These recommendations will be based on current scientific knowledge; data-protection and cybersecurity standards for processing AI training data; and debates about the maintenance of human control, human-in-the-loop, and/or human intervention during decision-making. The session will analyze in depth what "human intervention" means in this context and will assess whether and how this can be realistically and meaningfully ensured.

Layout by bakform.lu | Printed on 100% recycled paper, certified as climate-neutral.

DigitHarium

European Convention Centre, Luxembourg City



1 Registration desk

2 Wardrobe

3 Breakfast, lunch and coffee break

4 Salle PL

Day 1		Cyber Range
Day 2	Morning	Civilianization of conflict
Day 2	Afternoon	Frameworks of analysis
Day 3	Morning	OSI and data protection

5 Salle GR

Day 1		Cyber Range

6 Salle CZ

Day 1		Cyber Range

7 Salle BE

Day 1		Cyber Range
Day 2	Afternoon	Documenting Digital Risk using OSI

8 Salle IT

Day 1		Cyber Range
Day 2	Morning	Software Layer
Day 2	Afternoon	Cloud
Day 3	Morning	Measuring Cyber Harm

9 Salle UK

Day 1		Cyber Range
Day 2	Morning	Network Layer
Day 2	Afternoon	Data Protection and Biometrics
Day 3	Morning	Digital services for people on the move

10 Salle FR

Day 1		Cyber Range
Day 2	Morning	Humanity and AI
Day 2	Afternoon	Satellite
Day 3	Morning	Digital Emblem

11 Salle HU

Day 1		Cyber Range

12 Salle PT

Day 2		Hackathon
Day 3		Hackathon

13 Salle SE

Day 2		Hackathon
Day 3		Hackathon

14 Salle DE

Day 2	Morning	Mapping Digital Risks and Harms
Day 2	Afternoon	Digital Risks for Children Affected by Armed Conflict
Day 3	Morning	Navigating Trust & Safety

15 Salle C

Day 1	Morning	Opening Cyber Range
Day 1	Afternoon	Closing Cyber Range
Day 2	Morning	Opening Symposium
Day 3	Afternoon	Keynote adress: 1st Panel / 2nd Panel / 3rd Panel

→ Complete schedule on page 4