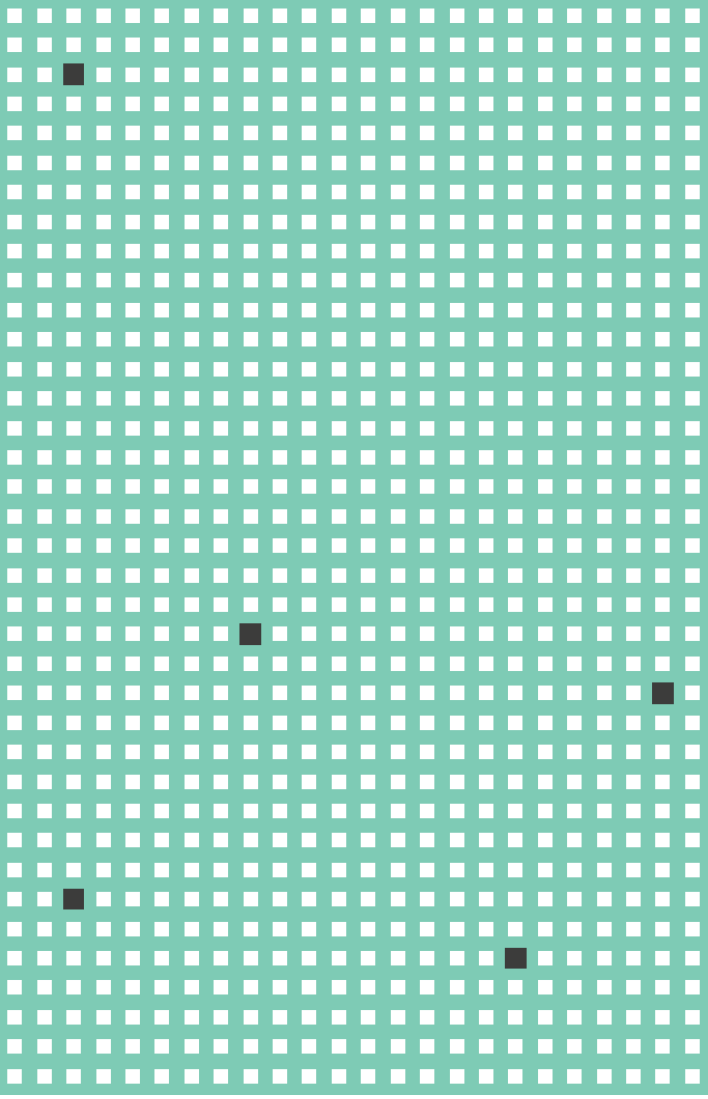

Symposium report

DIGITAL RISKS IN SITUATIONS OF ARMED CONFLICT

CODENODE LONDON UK
11-12 DECEMBER 2018

Acknowledgments

This report aims to capture the discussions and insights gained during the Symposium on Digital Risks for Populations in Armed Conflict. The Symposium was organized by the International Committee of the Red Cross (ICRC) and took place at CodeNode in London (UK) on 11th and 12th of December 2018.

The Symposium was organized by Delphine van Solinge and co-designed with Lisa Rudnick (Principal at The Policy Lab) and Joseph Guay (Director of research at The Do No Digital Harm Initiative). Artistic performances and pieces were managed by Philippe Stoll, whose team is also behind the joint ICRC and Privacy International report on Humanitarian metadata. Gabriel Mallows was the Master of Ceremonies.

This event would not have been possible without the support and significant contributions of the following ICRC staff members: Aduu Joba, Caroline Khoubesserian, Charlotte Lindsey Curtet, Delphine van Solinge, Eleonore Lecointe, Michael Mazliah, Philippe Stoll, Samuel Smith, Silvia Pelucchi, and Tina Bouffet. We also wish to thank the dozens of invited speakers and facilitators who came to London from various countries, as well as the 170 people who actively participated in the intensive two-day discussions.

This report was prepared by Delphine van Solinge, Tina Bouffet, and Silvia Pelucchi. The authors wish to thank the following Master's students from the London School of Economics for their note-taking during the event: Ann Marie McKenzie, Emily Featherstone, Maud Lampreia, Natalie Cilem and Patricia Olle. We also thank Jenny McAvoy, Ron Diebert, Gary Brown, Nathaniel Raymond, Charlotte Lindsey Curtet, Daniel Stauffacher and Pierre Gentile for their written contributions, and Joseph Guay and Lisa Rudnick for their incredible work.

This report does not necessarily reflect the official opinion of the ICRC or any of the event participants or facilitators. Responsibility for the information and views expressed in the report lies entirely with its authors.

TABLE OF CONTENTS

Foreword

"Whilst major conflicts are mainly happening in the physical world with kinetic power, **new technologies are rapidly giving rise to unprecedented methods of warfare and digital risks.** Among other things, these include side-effects of digital data experimentation, privacy violations, cyber-attack on critical infrastructures, disinformation campaigns on social media platforms and the mishandling of sensitive information that accompanies the humanitarian sector's efforts to deploy emerging technologies in already fragile contexts.

Today, it is not enough to understand only the physical environment of armed conflict. It is essential to overlay this with readings of the virtual or digital environment. The reality is that information online can dramatically affect **people's perceptions of what is happening off-line,** and vice versa. In a world that is increasingly connected, the spread of information and dis-information is having a dramatic impact on an individual or communities sense of security and safety.

Men, women, and children already living in insecure environments are particularly **susceptible to disinformation,** especially of the instantaneous nature and volume of that circulating on e.g. social media platforms. When lives and livelihoods depend on being able to read the security environment, it becomes vitally important to recognize that off-line and on-line are increasingly intertwined.

Images and information showing or purporting to show violence, incitement to hatred and conflict online are having real world impacts. In a highly politicized, polarized or weaponized environment, **misinformation and the propagation of content that can spread violence can be lethal.** Fact checking is hard at the best of times. But in situations of armed conflicts, it can be near impossible – especially in the real time within which people need to make the decisions to stay or flee.

Yet, the ICRC Symposium highlighted **that 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. It was identified that there is a knowledge gap between the technology and humanitarian sectors, and especially those working amongst populations that may have little knowledge of 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. The Symposium also guarded against generic digital literacy models and training. R**isk assessments need to be carried out with the affected populations in order to understand their needs and digital behaviors:** how they use their devices and the technologies they contain, and for what purpose. Thus, digital literacy programmes can and should be grounded on an evidence-based need and risk assessment.

In focusing on the digital risks for populations in armed conflict, experts at the ICRC Symposium looked at how such digital risks manifest themselves and what consequences these have for affected populations and those organizations who try to serve them. The three main scenarios discussed on the first day were: **(a) Surveillance, monitoring, and intrusion; (b) The weaponisation of information;** and, **(c) Cyber operations.**

The use and misuse of data was a strong theme throughout the discussions. Speakers highlighted the concerns with how data is collected, aggregated, accessed, analyzed, spread and even manipulated which is affecting the risks to individuals who would not see themselves as part of a conflict or battlefield. It was noted that the use of technologies to bring efficiency and scale in humanitarian responses

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, security of systems, and the identification of risks to individuals in order to be able to take appropriate mitigating action.

Unsurprisingly, in the field of Artificial Intelligence (AI) some key issues are already emerging such as data aggregation and **analysis of information on individuals which can heighten the risk for potential targeting of certain minorities or groups**. Another limitation of AI highlighted was that of bias, e.g. in facial recognition where systems have been trained on data sets that are predominantly biased towards certain characteristics. Such distortions or biases inherent in the training of systems must be corrected to enable their use. This is not simple.

During the Symposium, the ICRC called for a humanitarian purpose driven use of data collected for humanitarian responses. This means **to collect data respecting the needs of affected people**, 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. This is a complex endeavor 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 supported by, 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 "weaponisation" of information. It was recognized that a dialogue across sectors is needed.

It is important to understand how to maintain trust in the digital age. To do so we must ensure that we keep humanitarian purpose and the people – that humanitarian organizations are there to assist and protect - firmly at the center of any developments in order to ensure the humanitarian response capacities do no harm in their application. This requires that we understand the risks, protection issues, ethical concerns, and challenges before building digital solutions and having a valid and important humanitarian purpose for developing a certain digital capability or using certain data. The Symposium recognized that peoples' lives depended on this."

> *"Experiment in labs, not on people"*
>
> ***Charlotte Lindsey-Curtet***
> *Director of Digital Transformation & Data, ICRC*

Charlotte Lindsey Curtet
Director of Digital Transformation and Data
International Committee of the Red Cross
February 2019

Executive Summary

> *"As we work to uphold the dignity of people affected by conflict in the real world, we must also work to preserve their dignity and agency in the digital arena."*
>
> ***Pierre Gentile***
> *Head of the Protection Division, ICRC*

On 11 and 12 December 2018, the International Committee of the Red Cross (ICRC) organized a Symposium on Digital Risks in Armed Conflict and Other Situations of Violence in London[1].

It brought together 170 participants from humanitarian agencies, governments, the private sector, academia, and civil society. The aim was to address these needs and more specifically to **develop a deeper understanding** of the relationship between digital risk and the protection of individuals and communities affected by armed conflict. Discussions tried **to identify areas for cooperative action to** enable humanitarian actors and their partners to **respond more effectively** and appropriately to protection needs.

Participants had the opportunity to touch upon a range of sub-topics and themes. These were (a) **Digital surveillance, monitoring, and intrusion** against crisis-affected populations, humanitarian organizations, and their civil society partners; (b) **The weaponisation of information in armed conflict** to incite violence, spread misinformation, target vulnerable populations, and erode the protective capabilities of local communities, humanitarian actors, and their partners; and (c) **Cyber operations,** mainly the use of cyber means and methods of warfare, and the risk that negatively affect critical civilian infrastructure.

Various issues, needs, and recommendations emerged from these thematic discussions. All of them are underpinned by a broader need to include affected people in the conversation.

01. The humanitarian sector needs to **further understand how digital technologies can be used as a weapon** against civilian populations, and how this can be integrated into protection analysis, practice and risk mitigation.

02. To that end, the humanitarian sector needs to strengthen synergies with tech and academic circles in order to **produce timely and comprehensive evidence-based research** looking to improve humanitarian practice**.**

03. The humanitarian sector needs to develop and **strengthen its knowledge of the digital landscape and tools** in which it is navigating - often blindly.

04. The humanitarian sector – but not only – needs to **rearticulate what the Do No Harm principle means in a digital age.**

05. The humanitarian sector needs to seriously **invest in the development of digital literacy programs and education in digital risks** both for affected populations and for humanitarian practitioners.

06. The humanitarian sector needs to **integrate established data protection practices**. Though strong guidance exists, it has yet to be fully and systemically implemented.

07. The humanitarian sector needs to **stop experimenting new technologies on affected populations** without having put in place necessary safeguards and conducted a proper risks assessment to reduce exposure to risks.

[1] For the purposes of this report, a **threat** has been defined as a natural or man-made occurrence or action that has or shows the potential to harm life, dignity, information, systems, the environment and/or property. A **risk** has been defined as the potential for an unwanted outcome as a result of threat factors taking advantage of vulnerable individuals, event, environment etc. as determined by its likelihood and the associated consequences

08. The humanitarian sector needs **to stop establishing partnerships with the private sector** without putting in place the necessary protective procedures and regulations that define the terms of agreement and protect people's data.

09. There is a need to **set-up an overarching mechanism to report and manage critical incidents** related to data breaches across the humanitarian sector.

10. The humanitarian sector needs to discuss the usefulness and feasibility to **establish Professional Standards for digital risks** bearing in mind that with the velocity at which technology evolves, this would require constant review and update.

11. The ICRC, in particular, needs to continue **providing legal interpretation of IHL principles in situations where armed actors engage in cyber and information warfare** with a view to ensuring that the protection that IHL affords to civilians is upheld when it comes to cyber operations.

12. The humanitarian sector needs to **invest in the development of a governance and accountability framework for humanitarian action in the digital age**, under the auspices of a recognized convening body such as the Inter-Agency Standing Committee (IASC).

13. With the view to keep moving these recommendations further and deeper, the sector could **establish a more permanent structure with sufficient authority for policy and standards setting** (e.g. a working group on digital risks in armed conflicts under IASC).

14. Donors need to **promote a rights-based agenda for the responsible use of technologies and data**. They need to commit that their funds and the data they request from humanitarian organizations is directed towards a "humanitarian purpose driven approach".

15. Finally, the sector and others should **hold to account private sector companies** for their role in the weaponisation of information, data brokerage, digital surveillance and immature innovation in situations of armed conflict.

Jenny McAvoy
Director of Protection, InterAction

"It is critically important that humanitarian organizations evolve and adapt. The misuse of digital information and communication platforms reflect the dynamics of armed conflict but with a sophistication and scale of impact for which we have not been prepared.

Whether overtly malicious or unintentional, harmful behavior in the digital realm can affect every aspect of life and now represents a critical driver of violence and human suffering. Also at stake is the trust of vulnerable people in our role as humanitarian actors. Without this trust, we cannot be effective humanitarians and, once we lose this trust, it will be very difficult to earn it again.

The magnitude of the challenge cannot be understated – yet we shouldn't allow ourselves to be dissuaded. On one hand, we need to exercise tremendous care. We need resist the temptation to adopt new technological applications in our own work without ensuring we're mitigating the risks they could trigger or exacerbate.

At the same time, we need to assert norms of humanity in the digital realm, expand the protection dialogue to engage influential actors in technology sectors, and codify enforceable protections in national and multi-lateral policymaking."

Why this Symposium?

Digital technologies have become increasingly ubiquitous in our lives. The way people and organizations work and interact is being profoundly transformed. This so-called **Digital Revolution** is not limited to the business sector or to connected citizens living in so-called peaceful or stable countries. Digital technologies are also spreading – with less control and fewer safeguards - to places experiencing political, economic and/or social instability or fragility.

In these contexts, they have the potential to **exacerbate or change conflict dynamics** or enable new methods of warfare. They provide States, non-State actors and other stakeholders with new ways and means to operate with one another but also with people. This impacts how these same actors can protect or restrict fundamental rights, manage security and wage war.

> *"We are undermining the 'Values of Geneva' through a relatively blind embrace of the potential Promises of 'Silicon Valley"*
>
> ***Nathaniel Raymond***
> *Professor at Jackson Institute, Yale University*

The digital transformation is also **changing the humanitarian sector** and the way it delivers and implements protection and assistance activities. It offers opportunities to improve the humanitarian response, for instance by facilitating two-way communication between humanitarian staff and people affected by crises. The digital transformation provides innovative ways of capturing and exploiting crisis information[2] alongside new forms of digital assistance and evidence-based interventions.[3]

However, the digital transformation has also increased the threat of intentional and unintended harm. These can include **cyber-attacks** that target life-saving critical infrastructure and communications systems. People living in conflict-affected areas are increasingly vulnerable to emergent and abusive forms of digital surveillance, electronic exploitation and the "weaponisation" of information[4]. Moreover, they can be exposed to harmful (and often unintended) side-effects of **digital data experimentation, privacy violations**, and the **mishandling of sensitive information** by multiple actors, including humanitarian organizations deploying emerging technologies in already fragile contexts.

The full scope and nature of digital threats deriving from the growing use of technology in conflict affected countries remains unclear. Yet, this clarity is essential in order to anticipate potential harm and associated humanitarian consequences. It is also key towards mapping implications for humanitarian organizations using technology to provide assistance; or carrying out protection activities in increasingly digitalized contexts.

Based on these observations, the International Committee of the Red Cross (ICRC) organized a Symposium on Digital risks in armed conflict in London on December 11th and 12th 2018. Its overall objective was to connect a wide array of experts from different fields and sectors in order to jointly and critically look into these issues.

---

[2] Human rights defenders and humanitarian practitioners have made use of the enhanced situational awareness and actionable information afforded by the digital age. Examples include: (1) Employing remote sensing tools for augmenting conflict early warning capacities and documenting human rights abuse; (2) Leveraging mobile data solutions for tracking the conditions, profiles, and routes of transit of displaced populations; (3) Exploiting meta data from call detail records to predict the spread of infectious diseases; (4) Harvesting social media for sentiment analysis and rumor tracking in fragile contexts; (5) Exploring the Internet of things for Machine to Machine and Machine to People sensing for logistics and supply chain management; (6) Deploying aerial robotics for surveillance of damaged locations and monitoring critical infrastructure.

[3] Information, once used as a means by which to coordinate the delivery of food, shelter, and health services in humanitarian emergencies, for example, is now a life-saving commodity in and of itself and, some would argue, a human right for populations affected by natural disasters and conflict such as refugees and IDPs.

[4] An umbrella term that includes a range of emergent phenomena, including: online disinformation campaigns; online hate speech; viral rumors and dangerous speech; information operations; computational propaganda; etc.

Aim and Objectives

The Symposium's overarching aim was to develop a deeper understanding of the relationship between digital risks and the protection of individuals and communities affected by situations of armed conflict and violence. Participants sought areas for cooperative action to enable humanitarian actors and their partners to respond more effectively and appropriately to protection needs in a digital era.

Different challenges emerge when digital technologies and their possible uses intersect with the protection of individuals and communities. To remedy these, the Symposium invited exploration around the principles, ethics, and (emerging) standards to guide humanitarian professionals; the normative and legal frameworks designed to protect civilian populations; and the practices and capabilities that animate humanitarian action.

The event's specific objectives were to:

- Provide participants with a **better view of the digital threat landscape** faced by conflict affected populations;
- Explore the **implications of this digital threat landscape** where humanitarian protection matters are concerned;
- Examine **emerging strategies and change agendas** to improve protection outcomes;
- Identify **opportunities** for joint action.

Event overview

In an effort to provide a multi-sectorial approach to the topic, the Symposium brought together 170 participants from various backgrounds and sectors including from humanitarian agencies and organizations, governments, the private sector, academia, and civil society. All the discussions were held under Chatham House Rule unless otherwise authorized by the speaker.

The Symposium was built around four sessions spread over a day and a half. Each session was designed so as to contribute to a progressive learning curve. The first day alternated lightning talks from experts with facilitated group exercises built around three tracks. Each track had a specifically designed threat scenario.

Lightning talks

Targeted Espionage by Ron Diebert, Director of Citizen Lab, Professor at University of Toronto

The Weaponisation of Information by Brittan Heller, Berkman Centre for Internet and Society

Cyber Operations in Armed Conflicts by Laurent Gisel, Senior Legal Adviser, ICRC

Tracks and Scenarios

Track A: Digital surveillance, monitoring & intrusion

- **Real case scenario:** Syrian refugees' mobile devices are compromised through a malware attack (presented by Rakesh Bharania, Tarian Innovation)
- **Real case scenario:** Ethiopian dissidents are identified at home when an Ethiopian media outlet abroad is compromised (presented by Bill Marzack, The Citizen Lab)

Track B: Weaponisation of information

- **Real case scenario:** Online information operations in the context of the Syrian civil war (presented by Tom Wilson, University of Washington)
- **Real case scenario:** Anti-Muslim disinformation against the Rohingya community in Myanmar (presented by Christopher Tuckwood, The Sentinel Project)

Track C: Cyber operations

- **Fictional scenario:** Cyber-attack on humanitarian information systems and critical infrastructures as part of the armed conflict between Fictionland and Fablestan (presented by Gary Brown, College of Information & Cyberspace, National Defense University)

The facilitated exercises aimed at fostering new insights and creating a more holistic view for participants as to the nature of the risks and the protection implications presented by the incidence of digitalization on both conflicts and humanitarian action. They also looked at whether protection practitioners were appropriately equipped to identify and address those risks; avoid creating additional digital harm; and ways to strengthen resilience among conflict-affected populations.

Panel discussion

The day closed with a panel discussion whereby five experts examined how digital transformation and innovation agendas can support or hinder humanitarian protection outcomes. These experts were:

- **Charlotte Lindsey-Curtet**, Director for Digital Transformation and Data, ICRC;
- **Androulla Kaminara**, Director for Africa, Asia, Latin America, Caribbean and Pacific, ECHO;
- **Kyla Reid**, Head of Mobile for Humanitarian Innovation and Digital Identity, GSMA;
- **Heather Leson**, Data Literacy Lead, IFRC;
- **Meg Sattler**, UN OCHA

The panel was moderated by **Joseph Guay**, Director of Research, Do No Digital Harm Initiative.

On the second day, participants spent the morning taking stock of the different insights gained. They then identified key areas that they felt warranted immediate attention by the different concerned sectors. Here, three experts engaged in an open and frank discussion on the challenges and duties to ensure appropriate protection for conflict affected populations in the digital age. These experts included:

- **Nathaniel Raymond**, Professor at Jackson Institute, Yale University;
- **Nathaniel Gleicher**, Head of Cybersecurity Policy, Facebook;
- **Jenny McAvoy**, Director of Protection, InterAction.

The panel was moderated by **Joseph Guay**, Director of Research, Do No Digital Harm Initiative.

A concluding session split participants into groups, and presented them with the following question for discussion: what was the most important thing that needed to be addressed in order to deliver responsible and effective humanitarian protection that accounts for the influence and use of digital technologies in conflict areas?

Artistic Performances & Cultural Interventions

To bring a more visual and sensorial experience to this event, the following interventions were organized:

- **Deep Blue Dream** by Superstition, a performance that exposes people to what happens when artificial intelligence starts digging into your personal life.

- **AI Facial Profiling Machine** by Maria Revuelta, a machine whose use reveals the complex and intangible automated processes of analysis and classification of the human being into typologies. In a nutshell, the machine uses algorithmic intelligence to infer an individual's ability to handle firearms, and predict potential danger based on their facial features.

- **The Glass Room Experience** by TacticalTech, an interactive experience which prompts people to think about how their data is generated, harvested, traded and sold every day.

Highlights & Key Themes

Throughout the Symposium, many important needs emerged requiring action towards ensuring a more responsible and appropriate protection response to conflict-affected populations in the digital age.

Digital surveillance, monitoring, intrusion

The lightning talk held by Ron Deibert and the scenarios on Syrian refugees and Ethiopian dissidents (respectively presented by Rakesh Bharania and Bill Marzack) unpacked some of the complexities of digital surveillance by State and non-State actors (e.g. spyware sent via email).

It also highlighted a feeling of **uncertainty** around digital spying. Participants underlined that unless one was an expert in this area, it was hard to know whether one's devices, networks or systems had been compromised and whether someone, somewhere could take control over them, dig into personal files and possibly use them against an individual or their close relations. The consequences for vulnerable people include but are not limited to: being arrested, facing ill-treatment, having their identity stolen and therefore being denied access to certain services, having their assets stolen, or being psychologically affected by the fear of being under surveillance.

These practices are mounting in scale due to their easy accessibility and pervasiveness – spying software being cheap and easy to obtain. This upwards trend is facilitated by a continued lack of clarity under various legal frameworks. Participants from the humanitarian sector were particularly vocal about the **lack of knowledge** around, and complexity to detect, digital surveillance and other related risks that might target affected populations and humanitarian organizations alike.

To mitigate this, some suggested tailor-made **digital literacy** training**, standards of care and protocols** when providing connectivity to vulnerable populations, and investment in **information security system** for humanitarian organizations.

ICRC & Privacy International Report on humanitarian metadata

During the event, the ICRC and Privacy International presented their joint report on- The humanitarian metadata problem: 'Doing no harm' in the digital era.

The report looks into the risks associated with humanitarian sector's generation or collection of metadata (an often ignored and largely unprotected type of data). Yet, metadata from someone's text messages could be used to infer their sleeping patterns, travel routines or frequent contacts. This can be used to identify, profile, monitor or target individuals, including those in conflict environments.

The report details what metadata are collected or generated when humanitarian organizations use telecommunications, messaging apps or social media in their work. While the report does not advocate for privacy or against surveillance, it demonstrates how surveillance risks could obstruct or threaten the neutral, impartial and independent nature of humanitarian action.

To remedy this, it 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 organizations to improve **digital literacy** among their staff, volunteers, and affected people themselves.

Access the report here, or watch the series of 1-minute video explainers.

Weaponisation of information

The lightning talk by Brittan Heller was complemented by scenarios on the White Helmets in Syria and the Rohingya community in Myanmar, respectively presented by Tom Wilson and Christopher Tuckwood. These focused on the age-old phenomenon of manipulating information or propaganda via new, highly conducive outlets: the Internet and social media platforms.

In contexts with lower levels of literacy and critical thinking towards digital content, social media platforms such as Facebook may be seen as synonymous with the internet. What is seen on these platforms is considered true, especially if it comes from friends or acquaintances. The sender is often seen as more trustworthy than the source.

> *"Computation will not solve the hate speech dilemma."*
>
> ***Brittan Heller***
> *Berkman Centre for Internet and Society*

Understanding how the online world spills over to, and impacts, the offline one is challenging but critical. The consequences for vulnerable people include but are not limited to: being arrested and subject to ill-treatment, being discriminated against and denied access to services, being subject to assault and incurring physical injuries, facing destruction of property, or being psychologically traumatized by the fear of being attacked. Disinformation tends to target the "group" than only one individual.

This track on the weaponisation of information also raised a number of questions and challenges such as: how to identify who is behind the spread of misinformation, hate speech, or organic rumors based on misinformation; what is the effectiveness of **counter narratives** and early warning systems; what are the mechanisms that could prevent harmful information from spiraling out of control; and who has the legal and moral **responsibility to take action** against it.

In light of the complexity of this phenomenon, responsibility to address and manage consequences remains ambiguous. Yet, participants noted that current technical tools to counter hateful content were limited in terms of impact. While Artificial Intelligence and machine learning are being developed to better detect and counter abusive content, there is still a long way to go. Here, participants expressed a need to define collaborative approaches among concerned sectors, including the creation of human networks to monitor, verify and counter disinformation. Investing in **digital literacy** and **digital risks education** for affected communities can also improve resilience and critical thinking regarding digital content.

Gary Brown
Professor of Cyber Law at the College of Information & Cyberspace
National Defense University

"Surveillance of humanitarian operations is a given in this age of pervasive and inexpensive technology. Much of that surveillance will be benign, but some might be used in ways counter to humanitarian goals.

It's therefore incumbent on humanitarian organizations to act responsibly in gathering and protecting data, both their own and that belonging to the people they serve, to ensure it isn't used to harm them.

The most recently recognized, and perhaps most dangerous, cyberspace-based threat is the abuse of information, whether through disinformation or targeted information campaigns, designed to inflame tensions, promote violence, or prolong armed conflicts.

States are just beginning to grapple with the legal and practical implications of encouraging free and open access to information while also trying to limit the very real effects of hateful speech."

Cyber-operations in armed conflicts

The lightning talk by Laurent Gisel and the scenario on *Fictionland vs Fablestan* (presented by Gary Brown) clarified what is meant by cyber-warfare, i.e. the use of data streams against computers, computer systems, connected devices, or networks, as a means or method of warfare during an armed conflict.

Cyber operations have been used in some conflicts, notably by the U.S. and U.K. against the Islamic State group, to support kinetic operations. These operations included intelligence gathering on certain individuals through the Internet, social media, and data analytics that could inform kinetic targeting.

Through a fictional scenario, participants were invited to discover how cyber-operations during armed conflict could, by compromising key infrastructures, lead to large scale consequences on the economy, public safety and civilian access to essential services such as food, health, and education.

Interesting elements that emerged from the discussion included the necessity to ensure robust and resilient civilian systems to resist attack and prevent data leakage; and the need to set up cyber incident response teams specially trained to respond in armed conflict situations. For the humanitarian sector, this also raised the question of **data collection, data sharing, information security** (including possible partnership with the cyber security sector to plan responding to incidents) **and the duty of care.**

Digital Transformation

A panel discussion was held around the digital transformation and innovation agendas in the context of humanitarian protection. The panel noted a kind of "infatuation" around digital technologies, driven by various factors: competition, efficiency, effectiveness, the "panacea syndrome", and not least, donor pressure. Humanitarian organizations have started to view the words "digital" and "innovation" as a means to a new Eldorado that would allow them to meet needs on the ground, faster, better and on a larger scale.

Yet, this view is rarely complemented by an appropriate technical understanding of technology; and the implications and risks derived from their use in conflict settings. These risks and implications include data breaches, insecure data sharing practices, the misuse of individual data for purposes other than those originally intended, digital exclusion, etc.

The panel expressed concerns around donor pressure to provide **disaggregated data** on people receiving aid, and the risks this may entail for people, particularly the not-so-informed and / or not-so consenting. Another concern regarded the **lack of skills and knowledge** to properly use and leverage digital technologies without creating further risks for affected populations.

While the digital transformation is, to a certain extent, inevitable today, there is a need to clarify and commit to the notion of **due diligence** over effectiveness. Humanitarian organizations in particular need to understand the **needs of populations** first, in order to tailor their use of technologies and minimize risks for individuals by conducting rigorous **protection and data protection risk assessments.** This is a must if organizations wish **to be accountable to affected populations.**

With regards to **protection standards** and to **data and data protection**, the ICRC has recently developed two guidance documents. The **Professional Standards for Protection Work** (third edition) constitutes a set of minimum but essential standards aimed at ensuring that protection work carried out by human rights and humanitarian actors in armed conflict and other

situations of violence is safe and effective.[5] This third edition takes into account the changes that have occurred in the environment in which protection actors operate including the rapid developments in information communication technology and concurrent growth in data-protection law for and provides comprehensive guidelines on protection information management.

The **Handbook on Data Protection in Humanitarian Action** which is a comprehensive reference on the interpretation of data protection principles in the context of humanitarian action, particularly when new technologies such as Clouds Computing, Biometric, or Messaging Apps are employed.[6] While it has no binding force, its consistent application by humanitarian practitioners should be able to provide better safeguards and processes around the collection, management, storage and sharing of individual data.

Digital Literacy

Digital literacy often came up as a priority action. While it might not be the panacea to all of the aforementioned risks and challenges, helping people (both those receiving aid and humanitarian practitioners) to adopt healthier and safer digital behaviors could support increased resilience and protection.

However, experts warned against generic digital literacy models and training. For the program to be effective, a risk assessment needs to be carried out jointly with affected people, in order to understand their needs and digital behaviors. This includes how they use their devices and the technologies they contain, for what purposes, and with what level of technical knowledge. Thus, digital literacy programs would be grounded on evidence-based needs and risk assessments. At this stage, there is no standard protocol or guidance as to how to carry out such an assessment, nor how to translate into an informed and appropriate response.

Daniel Stauffacher
Founder & President, *ICT4Peace*

"Digital surveillance, the weaponisation of information, and cyber operations in armed conflict negatively impact the security and stability of societies and undermine democracies in peace time. How can we secure individuals' rights, data and privacy online, preventing disinformation and hate speech, using traditional national security approaches when the challenges we face are inherently both local citizen-based, and international?

We need to develop policies that consider more the individual as the epicenter of the security challenge instead of only traditional territorial sovereignty, even in Peace Time. Human beings need to be the core focus of the IT and security agenda going forward. That is why we have coined the term „Digital Human Security". Unfortunately we do not have an appropriate Forum for discussion in a structured and truly multi-stakeholder fashion, including in particular the Private Sector, who owns and runs IT infrastructure and the new age social media platforms."

Legal Framework

In recent years, prominent cyber-attacks have been reported in various countries, affecting the functioning of electricity networks and medical facilities, among others, and the delivery of such essential services to the population. While these hostile uses of cyberspace did not have large-scale humanitarian consequences, they are a stark reminder of the vulnerability of critical

[5] ICRC Professional Standards for Protection Work, 2018, https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

[6] ICRC Handbook on Data Protection in Humanitarian Action, 2017, *https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html?___store=default*

civilian infrastructure to cyber-attacks.[7] Meanwhile, disinformation campaigns and online propaganda have fused on social media, leading to increased tensions and violence against and between communities.

While the international community has asserted for several years that international law applies to cyber space, debates continue to arise on the relevance and adequacy of specific bodies of international law, including International Humanitarian Law (IHL). Are they sufficient? Do they need updating? Do they leave out gaps?

For the ICRC, there is no question that IHL applies to and restricts the use of cyber capabilities as a means and methods of warfare during armed conflicts, as it does with the use of any other new technology during conflicts. This position is also held by an increasing number of States.

Crucially, during armed conflicts, IHL prohibits cyber-attacks against civilian objects or networks, including notably cyber attacks against critical civiling infrastrucutre and the cyber infrastrucutre they rely on. IHL prohibits indiscriminate and disproportionate cyber-attacks. IHL also requires belligerents to take all feasible precautions to avoid incidental civilian harm when carrying out cyber-attacks and to protect civilians and civilian objects under their control from the effects of cyber operations.

In 2015, the ICRC published its views on the interpretation of IHL with regard to cyber operations during armed conflicts, and the challenges that it raises.[8] Among other issues, the ICRC includes references to cyber operations when updating the commentaries to the 1949 Geneva Conventions and their 1977 Additional Protocols.[9] The ICRC also acted as an observer for the drafting of the first edition of the Tallinn Manual (2013), whose academic endeavor is to bring light on the international law applicable to cyber warfare[10].

Ron Deibert
Director, *The Citizen Lab*

"Digital technologies bring many benefits and opportunities to humanitarian operations. However, the use of digital technologies by humanitarians carries with it a variety of important risks.

Zones of conflict in which humanitarian organizations operate are now highly-contested sites of struggle, including struggles in and through the information environment. Humanitarian organizations collect, store, share, and analyze data that is attractive to parties to armed conflict. The means to engage in information operations are widespread, growing, sophisticated, and widely available.

As a result, humanitarian organizations are exposed to a growing wave of digital attacks and cyber espionage, and have become highly prized targets. It is imperative that these organizations take digital security seriously as part of their core mission."

Applying pre-existing IHL rules to new means and methods of warfare raises the question of whether the rules are sufficiently clear in light of the specific characteristics of cyber and information warfare and their potential human cost for civilian population affected by armed conflicts. States that develop cyber military capabilities must ensure that such capabilities

[7] The ICRC organized in November 2018 an expert meeting on the potential human cost of cyber operations. The meeting report will be published in 2019.
[8] For more information see ICRC, "*International humanitarian law and the challenges of contemporary armed conflicts*" 31 October 2015, pp 39-44, as well as more generally ICRC website page on cyber warfare.
[9] See e.g. 2016 Commentary on the First Geneva Convention, paras 253-256 on Common Article 2 and paras 436-437 on Common Article 3. Cyber operations will be particularly relevant when updating the commentaries to the latter, which will be published in a few years
[10] See details on second edition here, and on our view upon the publication of the first version here.

can be used in accordance with international law,[11] which also requires clarity with regard to how the law applies[12].

Protection of civilians

The last day tried to tie conversations together by refocussing on the core theme of the conference: how to ensure an appropriate protection response for people affected by conflict and other violence in a digital era. An open and frank debate among three key experts helped to unearth important challenges and call certain people to take action. If no measures are taken rapidly, the debate underscored, the biggest scandal awaiting the humanitarian sector will concern **affected people's data** – how it is collected, used, processed, shared, leaked or monetized.

Root causes of the scandal would include practitioners' negligence with regards to data and the do no harm principle, the growing complacency towards a system of beneficiaries' data brokerage, private sector partnership without robust and protective regulations in place as well as a lack of common understanding of the duty of care. The fallout would likely have massive consequences on affected people, but also on trust, liability, and accountability within the sector.

With regards to data protection, recent years have allowed for the development of an increasingly robust and relevant body of laws. However, compliance with these legal standards poses considerable challenges.

The recently adopted European Union General Data Protection Regulation (GDPR) and the modernized Council of Europe Data Protection Convention have set the highest standards, placing a host of obligations on data controllers and processors. For the first time, these instruments recognize the challenges of processing and protecting personal data in humanitarian contexts, though they do not exempt humanitarian actors from complying with core data protection principles and requirements.

Data protection law is also spreading rapidly from Europe to the rest of the world. More than 100 countries now have some form of data protection law or sectorial privacy requirement, and new legislation is appearing all the time. This poses a significant challenge to humanitarian organizations, particularly where data is shared and/or transferred across borders and subject to overlapping legal regimes. However, legal frameworks on data protection exist, as well as specific guidance. It is crucial that humanitarian organizations take the necessary measures to implement them diligently.

Beyond data protection, however, there is a feeling that there is no clear mechanism or strong framework that enforces compliance with the duty of care and enables accountability with regards to responsible innovation. The **legal and shared responsibility** for our actions and decisions needs to be addressed. With this, there is an urgent need for the humanitarian sector to 1) review past and current actions and practices with regards to the use of digital technologies, data and partnerships 2) define the scope and modalities of the Do No Harm principle and due diligence obligations and "get its house in order".

Meanwhile, tech, government, and the private sector should also review their practices and how these impacts on people's lives.

[11] See Art. 36 of the 1977 First Additional Protocol.

[12] In this regard, the Commitment of the Commonwealth of Heads of Government to 'move forward discussions on how applicable international humanitarian law, applies in cyberspace in all its aspects' is welcome. See: *Commonwealth Cyber Declaration*, London, 20 April 2018: https://www.chogm2018.org.uk/sites/default/files/Commonwealth%20Cyber%20Declaration%20pdf.pdf

Nathaniel Raymond
Professor at Jackson Institute, *Yale University*

"First, the sector needs to define and publicly declare what ethical and legal obligations, including a duty of care, we have to communities whose data we collect, process, and share as part of operations. These obligations should be rooted in an official commentary from the ICRC that interprets how IHL and international human rights law applies to these activities. The commentary should also include a clear statement on when the provision of information constitutes protected and accepted humanitarian aid.

Second, we need to establish a critical incident management system for when data and ICT-related activities cause harm to communities. At present, we lack evidence for when risks become harms, and lack accountability to report when activities by humanitarians may have caused negative consequences. We can't do no harm if we don't know the harm. An independent review of critical incidents - including integration into M/E frameworks by donors - is a necessary first step.

A concern I have is that we, the humanitarian sector, have adopted a "humanitarian innovation" narrative. This narrative drives how we do our work before we have the time and space to develop protection frameworks, minimum technical standards, and coordination structures that are fit for purpose and consistent with humanitarian principles. Thus, we are undermining the "Values of Geneva" through a relatively blind embrace of the potential "Promises of Silicon Valley".

Living the principles of independence, neutrality, impartiality, and most importantly, humanity in the digital age requires us to treat "humanitarian-corporate" relations with similar safeguards and intentional distinction between actors similar to "civil-military" relations. To date, we have blithely, I think, assumed that humanitarians and private sector actors in the data space are on the same team. We are not and we must ensure that this difference is formally delineated and maintained.

The key recommendation coming out of the Symposium is that donors need to convene in 2019 to holistically and specifically discuss the role that they do play and should play in supporting and incentivizing the overall professionalization of how humanitarians utilize data and ICTs in complex contexts.

So far, there have been several wasted opportunities, most notably the 2016 World Humanitarian Summit, to develop a comprehensive and visionary donor agenda to support a responsible digital transformation in the sector.

Instead, there has been a strong drive towards "innovation" and "data-ification" of response without proportional and corresponding resources for doing so in a way consistent with humanitarian principles, ethics, law, and values. It is time for a donor summit that helps to put innovation "cart" squarely behind the horse of "protection".

Until the donors endorse and fund a rights-based agenda for the responsible use of data, humanitarians cannot succeed in using these now mainstream digital tools in a responsible, ethical and professional manner.

Futures & Recommendations

The following recommendations are all underpinned by a broader need to meaningfully include affected people in conversations around digital risks they may face.

01. The humanitarian sector needs to develop its **understanding of how digital technologies can be used as a weapon** against civilian populations, and how such threats and risks need to be integrated into protection analysis, practice and mitigation efforts.

02. To this end, the humanitarian sector needs to strengthen **healthy** synergies with tech and academic circles in order to produce **timely and comprehensive evidence-based research**. This research should look to improve humanitarian practice when digital technologies are misused in armed conflicts, impacting both affected populations and humanitarian organizations. A research group bringing together academics, humanitarians and technicians could be established to look specifically into these issues from an operational perspective.

03. The humanitarian sector needs to develop and strengthen its **knowledge of the digital landscape and tools** in which it is navigating - often blindly. Before using a new technology, humanitarian organizations must be able to fully appreciate the possible externalities for affected population and for themselves. If an organization does not have the knowledge in-house, external support has to be sought. To that end, there is a need to **develop meaningful synergies** across sectors to foster knowledge sharing and improve practice.

04. The humanitarian sector – but not only – needs to rearticulate what the **Do No Harm principle** means in a digital age. This implies evaluating what the use of digital technologies entails in terms of risks; exploring how to (responsibly) mitigate these risks; defining what kind of accountability mechanisms need to put in place, and anticipating possible remedial actions should things go wrong. This work could be carried out under the auspices of the IASC but not only.

05. The humanitarian sector needs to seriously invest in the development of **digital literacy programs and education in digital risks both for affected populations and for their staff.** In order to be meaningful, these would require tailored-made approaches based on the needs and behaviors of different populations. This, in turn, requires making use of risk assessment tools in order to identify the needs.

06. The humanitarian sector needs **to integrate established data protection practices** such as data minimization, data protection impact assessments, data protection by design and data subject's rights. Some humanitarian organizations have developed toolkits[13]. Data Protection Authorities websites [14] can also be a very good source of information and tools.

07. The humanitarian sector needs to **stop experimenting new technologies** on affected people without having previously put necessary safeguards in place, and conducted proper risks assessment to reduce risk exposure.

08. The humanitarian sector needs **to stop establishing partnerships** with the private sector without having put in place the necessary protective procedures and regulations that define the terms of the agreement and protect people's data.

09. There is a need to set-up an **overarching mechanism to report and manage critical incidents related to data breaches** in the humanitarian sector. This would allow for a

[13] *https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management*
https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html?___store=default

[14] https://www.cnil.fr/ , https://ico.org.uk/ or https://www.oaic.gov.au/ and many others

better understanding of what types of risks are being generated, and with what possible consequences for affected populations, so as to better mitigate them in the future. The structure, functioning, and credibility of such a mechanism will have to be carefully thought through as otherwise, organizations might prove reluctant to report incidents.

10. The humanitarian sector needs to discuss the usefulness and feasibility of establishing **Professional Standards for digital risks**, bearing in mind that with the velocity at which technology evolves, this would require constant review and update.

11. The ICRC, in particular, needs to continue **providing legal interpretation of IHL principles in situations where armed actors engage in cyber and information warfare** with a view to ensuring that the protection that IHL affords to civilians is upheld when it comes to cyber operations.

12. The humanitarian sector needs to invest in the development of a **governance and accountability framework for humanitarian action in the digital age**, under the auspices of a recognized convening body such as the Inter-Agency Standing Committee (IASC).

13. With the view to further these recommendations, **a more permanent structure** with sufficient authority **for policy and standards setting** could be established such as under IASC (e.g. a working group on digital risks in armed conflicts).

14. Donors need to **promote a rights-based agenda for the responsible use of technologies and data**. They need to commit that their funds and the data they request from humanitarian organizations is directed towards a "humanitarian purpose driven approach".

15. **Private sector companies need to be held accountable** for their role in the weaponisation of information, data brokerage, digital surveillance and immature innovation in situations of armed conflict.

Thinking and working collectively across sectors over two consecutive days was key towards better understanding and addressing critical issues facing affected people and humanitarian organizations in the digital age. However, much remains to be done – outside and within the humanitarian system at large – in order to fully comprehend the risks and address the harms that derive from the use of digital technologies by humanitarian practitioners and third parties.

As we move forward, it is crucial to maintain the centrality of protection in the digital age. This requires, among other things, solid commitments towards and investments in remedying knowledge, practice, skills, and resource gaps in an honest and collaborative manner. It also requires providing as safe space for affected populations to be part of those conversations and to have agency on those approaches and processes.

While the fear of reputational disgrace can be a driver of change, it is above all **the duty of care and do no harm principle towards affected people** that should push practitioners to correct and mitigate the risks that are taken when they use new technologies in their work.