SYMPOSIUM REPORT

DIGITAL RISKS IN ARMED CONFLICTS

CODENODE, LONDON, UK
11–12 DECEMBER 2018

REPORT

ICRC

SYMPOSIUM REPORT

DIGITAL RISKS IN ARMED CONFLICTS

CODENODE, LONDON, UK
11–12 DECEMBER 2018

ACKNOWLEDGEMENTS

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 11 and 12 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 organized 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 drawn up 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 would also like to thank Jenny McAvoy, Ron Deibert, 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

Although major conflicts are still fought primarily in the physical world through kinetic operations, **new technologies are rapidly giving rise to new methods of digital warfare** – in the form of cyber attacks on critical infrastructure or disinformation campaigns on social media, for instance – **and increased risk, such as privacy violations and the mishandling of sensitive information.** The humanitarian sector can itself heighten these risks as it seeks to try out new technologies in already fragile contexts.

Today, it is just as important to understand the virtual and digital environment in which armed conflicts occur, as it is the physical context. The reality is that **online information can dramatically affect people's perceptions of what is happening offline,** and vice versa. In a world that is increasingly connected, the spread of information and disinformation can have a major impact on an individual or community's sense of security and safety.

Men, women and children already living in dangerous environments are particularly susceptible to disinformation, especially when it appears instantaneously and in great volumes on social media. When lives and livelihoods depend on being able to gauge the security environment, it becomes vitally important to recognize that the offline and online worlds are increasingly intertwined.

Online images and information showing or purporting to show violence, incitement to hatred and conflict can have real-world impacts. In a highly politicized, polarized or weaponized environment, **misinformation and other content that incites violence can be lethal.** Fact-checking is hard at the best of times. But in situations of armed conflict, it can be near impossible – especially in the short time that people have to make the decision to stay or flee.

Yet one outcome of the ICRC symposium held in December 2018 was that **focusing on content alone is not enough**; it is also important to focus on ensuring that mechanisms are in place to prevent online discussions from escalating to a point where they become harmful.

The people that humanitarians work with – and the humanitarians themselves – may not have a good grasp of the technology. **Populations with a low level of digital literacy tend to believe what they see on social media**, and they may have little knowledge of how technology can work for or against them. It is therefore important to raise levels of digital literacy in order to increase the resilience of those communities and ensure they are better protected. But experts at the symposium guarded against generic digital literacy models and training. Instead, **digital literacy programmes can and should be built around evidence-based needs and risk assessments, which can be carried out within affected communities in order to understand their needs and digital behaviours.**

Experts at the symposium also looked at how digital risks manifest themselves and what consequences they have on affected populations and the organizations that serve them. **The three main topics discussed on the first day were: surveillance, monitoring and intrusion; the weaponization of information; and cyber operations.**

The use and misuse of data was a strong theme throughout the discussions. Speakers expressed concerns about how data are collected, aggregated, accessed, analysed, spread and even manipulated, and how that can increase the risks to individuals who may not see themselves as part of the conflict. They also noted that technologies are increasingly being used to enhance the efficiency and scale of humanitarian responses, often without due diligence. Yet **it is essential to conduct due diligence before adopting new technologies** in order to determine the risks to individuals and the potential impact on privacy and system security. Only then can appropriate mitigating action be taken.

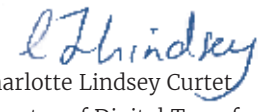
Unsurprisingly, the use of artificial intelligence has already raised a number of issues – **data aggregation and information analysis can, for instance, heighten the risk of certain minorities or groups being targeted,** while facial recognition systems are trained using data sets with a bias towards certain facial features. Such distortions or biases inherent in the training of systems must be corrected before these technologies can be used – and that is no easy task.

During the symposium, the ICRC called for data collection to be driven by humanitarian needs and have a humanitarian purpose. As such, **data should only be collected if it will improve the response provided to conflict-affected people;** data collection should be kept to the strict minimum even if the technology allows much more data to be collected than is necessary for effective programming; and the need for policies and consent as to how data can be used should be recognized. This is a complex undertaking requiring investment in understanding what people affected by armed conflict need, what risks they are exposed to, what makes them more vulnerable to those risks, and what specific technological characteristics and capabilities could actually cause more harm than good when used in situations of conflict.

As conventional ways of conducting armed conflict are reinforced, transformed and replaced by digitally derived forms of violence, persecution and exploitation, **those affected by conflict or other situations of violence become vulnerable in different ways** as well. They might have to contend with cyber attacks on life-saving critical infrastructure and communications systems or with new, more subtle forms of digital surveillance, electronic exploitation, and the "weaponization" of information. Yet these issues can only be addressed if all sectors are included in the conversation.

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

Finally, maintaining the trust of those we serve as we make increasing use of digital technologies will be crucial. We must therefore keep our humanitarian purpose and the people we are there to help and protect firmly at the centre of our work – this will help to ensure that any use of digital technology does not cause harm. And before adopting a digital solution, we must be sure that we fully understand the risks, protection-related issues, ethical concerns and challenges involved and that the solution serves a clear humanitarian purpose. After all, peoples' lives will depend on this.



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

EXECUTIVE SUMMARY

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]

> *"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*

The event was attended by 170 people from humanitarian agencies, governments, the private sector, academia and civil society. The aim of the symposium was to **assess the digital risks** arising out of armed conflicts and **develop a deeper understanding** of how to protect conflict-affected individuals and communities from those risks. Discussions focused on identifying areas in which cooperation could be strengthened to **increase the effectiveness of the protection work** conducted by humanitarian organizations and their partners.

Participants also held discussions on a range of sub-topics and themes. These were: **digital surveillance, monitoring and intrusion** involving crisis-affected populations, humanitarian organizations and their civil society partners; the **weaponization of information in armed conflicts,** with the aim of inciting violence, spreading false information, targeting vulnerable populations and eroding the ability of local communities, humanitarian organizations and their partners to protect themselves; and **cyber operations,** with a focus on the use of cyber warfare and the resulting risks to critical civilian infrastructure.

Various issues, needs and recommendations emerged from these thematic discussions, and the broader need to include affected people in the conversation was also highlighted. The conclusions were as follows:

1. The humanitarian sector needs to **gain further insight into how digital technologies are used as a weapon** against civilian populations, and consider how that insight can be integrated into protection-related analyses, practices and risk mitigation.
2. 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** that looks to improve humanitarian practices.
3. The humanitarian sector needs to develop and **strengthen its knowledge of the digital landscape** in which it navigates – often blindly.
4. The humanitarian sector – along with other sectors – needs to **rethink what the "do no harm" principle means in the digital age.**
5. The humanitarian sector needs to **invest substantially in the development of digital literacy programmes and training on digital risks,** both for affected populations and for humanitarian practitioners.
6. The humanitarian sector needs to **integrate established data-protection practices** into its work. Although strong guidance exists, it has yet to be fully and systematically implemented.

1 For the purposes of this report, a **threat** is as a natural or man-made occurrence or action that has the potential to harm life, dignity, information, systems, the environment and/or property. A **risk** is a potentially unwanted outcome as a result of a threat that takes advantage of vulnerable individuals, events, environments etc. as determined by its likelihood and the associated consequences.

7. The humanitarian sector needs to **stop testing new technologies on affected populations** without first putting in place the necessary safeguards and conducting a proper risks assessment to reduce exposure to risks.

8. The humanitarian sector needs to **stop entering into partnerships with the private sector** without first putting in place the necessary protective procedures and regulations setting out the terms of the agreement and ensuring that people's data are protected.

9. **An overarching mechanism is needed to report and manage critical incidents** related to data breaches across the humanitarian sector.

10. The humanitarian sector needs to discuss whether it would be useful and feasible to **establish professional standards for digital risks,** bearing in mind that the fast pace of technological change means that such standards would need to be constantly reviewed and updated.

11. The ICRC, in particular, needs to **continue providing legal interpretations of international humanitarian law in situations where armed groups engage in cyber and information-related warfare,** with a view to ensuring that international humanitarian law continues to protect civilians affected by 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. In order to strengthen these recommendations, the sector could **establish a more permanent structure with sufficient policy-making and standard-setting authority** (e.g. a working group on digital risks in armed conflicts under the IASC).

14. Donors need to **promote a rights-based agenda for the responsible use of technologies and data.** They need to ensure that the use of funds and their requests for data from humanitarian organizations are guided by a humanitarian purpose.

15. Finally, **private-sector companies need to be held accountable** for their role in the weaponization of information, data brokerage, digital surveillance and immature innovation in armed conflicts.

JENNY MCAVOY
DIRECTOR OF PROTECTION, INTERACTION

"It is critically important that humanitarian organizations evolve and adapt. The misuse of digital information and communication platforms reflects 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 behaviour 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 multilateral policy-making."

WHY THIS SYMPOSIUM?

Digital technologies have become increasingly ubiquitous in our lives. And the way people and organizations work and interact has changed enormously. This so-called digital revolution is not limited to the business sector or to connected citizens living in peaceful or stable countries. Digital technologies are spreading – with less control and fewer safeguards – to places experiencing political, economic and/or social instability and fragility.

These technologies have the potential to exacerbate or change the dynamics of a conflict and to enable new methods of warfare. They provide States, non-State entities and other stakeholders with new ways of operating and means of working with one another as well as with civilians. And this has an impact on how they 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 provides protection and assistance. Digital technologies offer ways to improve the humanitarian response – for instance by facilitating two-way communication between humanitarian staff and people affected by crises – and of capturing and exploiting crisis-related information.[2] They also bring new forms of digital assistance and evidence-based interventions.[3]

However, the **digital transformation has also increased the threat** of intentional and unintentional harm; intentional harm could, for instance, take the form of **cyber attacks** that target life-saving infrastructure and communications systems. People living in conflict-affected areas are increasingly vulnerable to new, abusive forms of digital surveillance, electronic exploitation and the "weaponization" of information.[4] They are also exposed to the harmful (and often unintended) side effects of **digital data experimentation,** may have their privacy violated or be left vulnerable as a result of the **mishandling of sensitive information,** including by humanitarian organizations deploying emerging technologies in already fragile contexts.

The full scope and nature of the digital threats deriving from the growing use of technology in conflict-affected countries remains unclear. Yet more needs to be known about those threats if we are to accurately gauge the harm they could potentially cause and the associated humanitarian consequences. Greater clarity

2 Human rights activists and humanitarian practitioners have made use of the enhanced situational awareness and actionable information provided by digital technologies. Examples include: employing remote sensing tools to increase early warning capacities and record human rights abuses; leveraging mobile data solutions to track the conditions, profiles and routes of transit of displaced populations; exploiting metadata from call detail records to predict the spread of infectious diseases; harvesting social media for sentiment analysis and rumour tracking in fragile contexts; exploring the internet of things for machine-to-machine and machine-to-people sensing in logistics and supply chain management; and deploying aerial robotics for the surveillance of damaged locations and the monitoring of critical infrastructure.

3 Information, once used as a means by which to coordinate, for example, the delivery of food, shelter, and health services in humanitarian emergencies, 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 internally displaced people.

4 An umbrella term that covers a range of new phenomena, including: online disinformation campaigns; online hate speech; viral rumours and dangerous speech; information operations; and computational propaganda.

is also key when it comes to mapping the implications for humanitarian organizations using technology to provide assistance or to conduct protection work in increasingly digitalized contexts.

The symposium was organized with the overall objective of bringing together an array of experts from different sectors in order to take a critical look at the issues described above.

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 armed conflict and other situations of violence. Participants looked for areas in which humanitarian organizations and their partners can work together in order to more effectively meet people's protection needs in the digital era.

There are various challenges that arise when considering the role that digital technologies can play in protecting conflict-affected people and communities. To address these challenges, symposium participants were encouraged to explore the principles, ethics and (emerging) standards that guide humanitarians in their work; the norms and legal frameworks designed to protect civilian populations; and the practices and capabilities that drive humanitarian activities.

The event's specific objectives were to:

- provide participants with a better overview of the digital threats to conflict-affected populations
- explore the implications of these digital threats with regard to humanitarian protection work
- examine new strategies and change agendas with a view to improving protection outcomes
- identify opportunities for joint action.

EVENT OVERVIEW

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

The symposium was broken down into four sessions spread over a day and a half. Each session was designed to build on what had been learned during the previous session. On the first day, lightning talks by experts were alternated with facilitated group exercises broken down into three tracks. Each track was based on a specifically designed threat scenario.

LIGHTNING TALKS

Targeted Espionage by Ron Deibert, Director of The Citizen Lab, Professor at the University of Toronto
The Weaponization 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 and intrusion

- **Real-life scenario:** A malware attack compromises Syrian refugees' mobile devices (presented by Rakesh Bharania, Tarian Innovation)
- **Real-life scenario:** An Ethiopian media outlet abroad is compromised, and Ethiopian dissidents are identified at home as a result (presented by Bill Marzack, The Citizen Lab)

Track B: Weaponization of information

- **Real-life scenario:** Online information-gathering operations in the context of the Syrian civil war (presented by Tom Wilson, University of Washington)
- **Real-life 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 infrastructure as part of the armed conflict between Fictionland and Fablestan (presented by Gary Brown, College of Information & Cyberspace, National Defense University)

The aim of the facilitated exercises was to provide participants with new, more comprehensive insights into digital risks and the protection-related implications for both conflicts and humanitarian action. Participants also looked at whether protection workers were appropriately equipped to identify and address those risks and avoid creating additional digital harm; they also considered ways to strengthen resilience among conflict-affected populations.

PANEL DISCUSSION

The day ended with a panel discussion in which five experts examined how digital transformation and innovation agendas can support or hinder humanitarian protection outcomes. The panel members 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 insights they had gained the previous day. They then identified key areas that they felt warranted immediate attention by the various sectors concerned. Here, three experts engaged in an open and frank discussion on the duties and challenges of providing appropriate protection for conflict-affected populations in the digital age. Those experts were:

- **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.

In the wrap-up session, participants were split into groups and presented with the following question for discussion: what is the most important thing that needs to be addressed in order to deliver responsible and effective humanitarian protection that takes account of the influence and use of digital technologies in conflict areas?

ARTWORK AND PERFORMANCES

To provide a more visual and sensory representation of the issues under discussion, the following artwork and performances were exhibited:

- **Deep Blue Dream** by Superstition, a performance that illustrates what happens when artificial intelligence starts digging into your personal life.
- **AI Facial Profiling Machine** by Marta Revuelta, a machine that reveals the complex and intangible automated processes of analysing and categorizing people. 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 that prompts people to think about how their data are generated, harvested, traded and sold every day.

HIGHLIGHTS AND KEY THEMES

During the symposium, participants identified a number of key areas requiring action in order to ensure a more responsible approach to protecting conflict-affected populations in the digital age.

DIGITAL SURVEILLANCE, MONITORING AND INTRUSION

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

It also **highlighted the feeling of uncertainty with regard to digital spying.** Participants underlined the fact that it was hard for people who were not experts to know whether their devices, networks or systems had been compromised and whether someone somewhere could take control of their devices, dig into their personal files and possibly use that information against them or those close to them. 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, and being psychologically affected by the fear of being under surveillance.

These practices are mounting in scale because spying software is cheap and easy to obtain. This trend is facilitated by the continued lack of clarity provided within legal frameworks. **Participants from the humanitarian sector were particularly vocal about how difficult digital surveillance is to detect and the lack of knowledge about that and other related risks** to affected populations and humanitarian organizations alike.

To mitigate this, **some participants suggested providing tailor-made digital literacy training, introducing standards of care and protocols** to be followed when providing connectivity to vulnerable populations, and investing in information security systems for humanitarian organizations.

ICRC & PRIVACY INTERNATIONAL REPORT ON HUMANITARIAN METADATA

During the event, the ICRC and Privacy International presented their joint report entitled "The Humanitarian Metadata Problem: 'Doing No Harm' in the Digital Era".

The report looks at the risks that arise when the humanitarian sector generates and collects metadata (an often ignored and largely unprotected type of data). Metadata from someone's text messages could, for instance, be used to infer that person's sleeping patterns, travel routines or frequent contacts. This, in turn, could be used to identify, profile, monitor or target individuals, including those in conflict environments.

The report provides details of the metadata that are collected and 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 work.

In response, it **recommends 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 one-minute video explainers.

WEAPONIZATION OF INFORMATION

The lightning talk by Brittan Heller was followed by scenarios involving the White Helmets in Syria and the Rohingya community in Myanmar, presented by Tom Wilson and Christopher Tuckwood respectively. These scenarios focused on the age-old phenomenon of manipulating information and propaganda, but this time using new, highly conducive outlets: the internet and social media.

In contexts where people have lower levels of digital literacy and think less critically about 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. What's more, disinformation tends to target the "group" rather than just one individual.

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

In light of the complexity of this phenomenon, it is still unclear who is responsible for addressing and managing the consequences. Yet participants noted that current technical tools to counter hateful content were limited in terms of their impact. Artificial intelligence and machine learning are being developed to better detect and counter abusive content, but there is still a long way to go. Here, participants expressed the need to come up with approaches that brought together the various sectors concerned, such as by creating networks of people to monitor, verify and counter disinformation. **Investing in digital literacy and training on digital risks for affected communities could 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 that run 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 to support kinetic operations in some conflicts, most notably by the US and UK governments against the Islamic State group. These operations involved using the internet, social media and data analytics to gather intelligence on certain individuals in order to inform kinetic targeting.

Through a fictional scenario, participants learnt more about how cyber operations during armed conflict could, by compromising key infrastructure, have large-scale consequences on the economy, public safety and civilian access to essential services such as food, health and education.

Interesting points that emerged from the discussion included the need to ensure that civilian systems were robust and resilient enough to withstand an attack and prevent data leakage, and the need to set up cyber-incident teams that are specially trained to respond in armed conflict situations. For the humanitarian sector, **this also raised questions about data collection, data sharing, information security (including possible partnerships with the cyber security sector to plan its response to incidents) and the duty of care.**

THE DIGITAL TRANSFORMATION

A panel discussion was held on the digital transformation and innovation in the context of humanitarian protection. The panel noted a kind of "infatuation" with 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 way of achieving 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 backed by an adequate understanding of technology, and the implications and risks derived from its use in conflict settings, which include data breaches, unsecure data-sharing practices, the misuse of individual data for purposes other than those originally intended, and digital exclusion.

The panel expressed concerns about the pressure exercised by donors to provide disaggregated data on the people receiving aid, and the risks this may entail for people, particularly those who are less well informed or have not given their consent. **Another concern regarded the lack of skills and knowledge of how 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, **the notion of due diligence needs to be clarified and to take precedence 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 risk assessments that also cover data protection. This is a must if organizations wish to be accountable to affected populations.**

The ICRC recently created two guidance documents in the areas of protection and data protection. ***Professional Standards for Protection Work*** (third edition) provides a set of essential minimum standards aimed at ensuring that the protection work carried out by human rights and humanitarian organizations 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 workers operate, including the rapid developments in information and communication technology and concurrent growth in data-protection law, and provides comprehensive guidelines on how to manage protection-related information.

The ***Handbook on Data Protection in Humanitarian Action***[6] is a comprehensive reference document on how to interpret data-protection principles in a humanitarian context, particularly when new technologies such as cloud computing, biometrics and messaging apps are employed. While the handbook is not binding, its consistent application by humanitarian practitioners would ensure there were better safeguards and processes for collecting, managing, storing and sharing 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 behaviours could increase resilience and enhance protection work.

However, experts warned against generic digital literacy models and training. For programmes to be effective, a risk assessment needed to be carried out jointly with affected people, in order to understand their needs and digital behaviours. This assessment should look at how they use their devices and the technologies they contain, for what purposes, and with what level of technical knowledge. Thus, digital literacy programmes would be built 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 that assessment into an informed and appropriate response.

5 ICRC, *Professional Standards for Protection Work carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence,* 3rd edition, Geneva, 2018: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

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

DANIEL STAUFFACHER
FOUNDER & PRESIDENT, ICT4PEACE

"Digital surveillance, the weaponization 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 and 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 epicentre 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 that allows for a structured and truly multi-stakeholder dialogue across sectors – including the private sector, which owns and runs IT infrastructure and new-age social media platforms."

LEGAL FRAMEWORK

In recent years, major cyber attacks have been reported in various countries, causing disruptions in electricity networks and at medical facilities, among others, and the delivery of essential services to the population. While these hostile uses of cyberspace did not have large-scale humanitarian consequences, they are a stark reminder of how vulnerable critical civilian infrastructure is to cyber attacks.[7] Meanwhile, disinformation campaigns and online propaganda have become more common 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 concerning the relevance and adequacy of specific bodies of international law, including international humanitarian law. Are they sufficient? Do they need updating? Do they leave gaps?

For the ICRC, there is no question that international humanitarian law 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 technologies during conflicts. This position is also held by an increasing number of States.

Crucially, during armed conflicts, international humanitarian law prohibits cyber attacks against civilian objects or networks, including cyber attacks against critical civilian infrastructure and the cyber infrastructure they rely on. International humanitarian law also prohibits indiscriminate and disproportionate cyber attacks, and it 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 international humanitarian law with regard to cyber operations during armed conflicts, and the challenges that it raises.[8] The ICRC has also included references to cyber operations when updating the commentaries to the Geneva Conventions and their Additional Protocols.[9] It also acted as an observer in the drafting of the first edition of the Tallinn Manual (2013), an academic document that seeks to shed light on the international law applicable to cyber warfare.[10]

7 In November 2018, the ICRC organized 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*, 2015, pp 39-44, as well as the ICRC webpage on cyber warfare.

9 See, for example, the 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 a key element of the next update to these commentaries, which will be published in a few years.

10 Details of the second edition are available here, and on our view of the first version can be found here.

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, and the struggle also takes place within and around the information environment. Humanitarian organizations collect, store, share, and analyse data that is attractive to parties to armed conflict. The means to engage in information operations are 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 the pre-existing rules of international humanitarian law to new means and methods of warfare raises the question of whether the rules are sufficiently clear given the specific characteristics of cyber and information warfare and their potential human cost for civilian populations affected by armed conflicts. States that develop cyber military capabilities must ensure that such capabilities are used in accordance with international law,[11] and be clear about how that law is applicable.[12]

PROTECTION OF CIVILIANS

The aim of the discussions on the last day was to try and tie everything together by once again focusing on the core theme of the conference: how to ensure that the protection response for people affected by conflict and other violence is adapted to the digital era. An open and frank debate among three key experts helped to unearth important challenges and call certain people to take action. If measures are not taken rapidly, the debate underscored, **the biggest scandal awaiting the humanitarian sector will concern people's data** – how it is collected, used, processed, shared, leaked or monetized.

Root causes of the scandal could include practitioners' negligence with regard to data and the "do no harm" principle, the growing complacency towards a system of data brokerage, private sector partnerships without robust and protective regulations in place, and a lack of a 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.

While an increasingly robust and relevant body of data-protection laws has been developed in recent years, ensuring compliance with these legal standards is a major challenge.

The recently adopted European Union General Data Protection Regulation (GDPR) and the updated Council of Europe Data Protection Convention have set high standards, placing a host of obligations on data controllers and processors. These instruments now recognize the challenges of processing and protecting personal data in humanitarian contexts, without exempting humanitarian organizations from their obligation to comply with core data-protection principles and requirements.

11 See Art. 36 of the First Additional Protocol

12 The Commonwealth of Heads of Government made a commitment to "move forward discussions on how applicable international humanitarian law applies in cyberspace in all its aspects". See: *Commonwealth Cyber Declaration*, London, 20 April 2018: https://www.chogm2018.org.uk/sites/default/files/Commonwealth%20Cyber%20Declaration%20pdf.pdf

Data-protection legislation is also being brought in in other parts of the world. More than 100 countries now have some form of data-protection law or sector-based privacy requirements, and new legislation is appearing all the time. This poses a significant challenge to humanitarian organizations, particularly when data are 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, the feeling is that there is no clear mechanism or strong framework to ensure compliance with the duty of care and ensure accountability with regard to responsible innovation. **Our shared legal 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 concerning the use of digital technologies, data and partnerships; and 2) define the scope and terms of the "do no harm" principle and due diligence obligations and "get its house in order".

Meanwhile, both the government and the private sector, and especially the tech sector, should review their practices and the impact they have on people's lives.

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 international humanitarian law and international human rights law apply 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 of when risks become harms, and lack accountability to report when activities by humanitarians may have caused negative consequences. We cannot "do no harm" if we don't know the harm. An independent review of critical incidents – including integration into monitoring and evaluation 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 an intentional distinction between them that is similar to that of 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 that supports a responsible digital transformation in the sector.

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

OUTLOOK AND RECOMMENDATIONS

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

1. The humanitarian sector needs to **gain further insight into how digital technologies are used as a weapon against civilian populations,** and consider how that insight can be integrated into protection-related analyses, practices and risk mitigation.

2. 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** that looks to improve humanitarian practices when digital technologies are misused in armed conflicts and when that misuse has an impact on civilian populations and humanitarian organizations. A research group bringing together academics, humanitarians and technicians could be established to look at these issues from an operational perspective.

3. The humanitarian sector needs to develop and **strengthen its knowledge of the digital landscape** in which it navigates – often blindly. Before using new technologies, 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, meaningful synergies need to be developed across sectors to foster knowledge-sharing and improve practices.

4. The humanitarian sector – along with other sectors – needs to **rethink what the "do no harm" principle means in the digital age**. This should involve 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 Inter-Agency Standing Committee (IASC) and other entities.

5. The humanitarian sector needs to **invest substantially in the development of digital literacy programmes and training on digital risks**, both for affected populations and for humanitarian practitioners. For these programmes to be meaningful, a tailor-made approach has to be taken, based on the needs and behaviours of different populations. This, in turn, would require risk assessment tools to be used in order to identify the needs.

6. The humanitarian sector needs to **integrate established data-protection practices** into its work. Such practices include data minimization, data protection impact assessments, data protection by design and data subject's rights. Some humanitarian organizations have already developed toolkits in this regard.[13] The websites of data-protection authorities[14] can also be a very good source of information and other tools.

7. The humanitarian sector needs to **stop testing new technologies on affected populations** without first putting in place the necessary safeguards and conducting a proper risks assessment to reduce exposure to risks.

8. The humanitarian sector needs to **stop entering into partnerships with the private sector** without first putting in place the necessary protective procedures and regulations setting out the terms of the agreement and ensuring that people's data are protected.

9. **An overarching mechanism is needed to report and manage critical incidents** related to data breaches across the humanitarian sector. This would allow for a better understanding of what types of risks are being generated, and the possible consequences for affected populations, so as to reduce the risks in the future. Such a mechanism would have to have a well-thought-out structure and organization and be credible so that organizations are not reluctant to report incidents.

10. The humanitarian sector needs to discuss whether it would be useful and feasible to **establish professional standards for digital risks**, bearing in mind that the fast pace of technological change means that such standards would need to be constantly reviewed and updated.

11. The ICRC, in particular, needs to **continue providing legal interpretations of international humanitarian law in situations where armed groups engage in cyber and information-related warfare**, with a view to ensuring that international humanitarian law continues to protect civilians affected by 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 IASC.

13. In order to strengthen these recommendations, the sector could **establish a more permanent structure with sufficient policy-making and standard-setting authority** (e.g. a working group on digital risks in armed conflicts under the IASC).

14. Donors need to **promote a rights-based agenda for the responsible use of technologies and data**. They need to ensure that the use of funds and their requests for data from humanitarian organizations are guided by a humanitarian purpose.

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

13 For instance, Oxfam and the ICRC
14 For example: CNIL, ICO and OAIC

Over the course of the two-day symposium, participants from across sectors were given the opportunity to work together to better understand and address the critical issues facing affected people and humanitarian organizations in the digital age. However, much remains to be done – both outside and within the humanitarian system – in order to fully comprehend the risks and address the harmful use of digital technologies by humanitarian practitioners and third parties.

As we move forward, it is crucial for protection to remain central in our work in the digital age. This requires, among other things, solid commitments towards and investments in narrowing knowledge, practice, skills, and resource gaps in an honest and collaborative manner. The humanitarian sector also needs to provide a safe space for affected populations to be part of those conversations and to have agency regarding the related approaches and processes.

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

The ICRC helps people around the world affected by armed conflict and other violence, doing everything it can to protect their lives and dignity and to relieve their suffering, often with its Red Cross and Red Crescent partners. The organization also seeks to prevent hardship by promoting and strengthening humanitarian law and championing universal humanitarian principles.

People know they can count on the ICRC to carry out a range of life-saving activities in conflict zones and to work closely with the communities there to understand and meet their needs. The organization's experience and expertise enables it to respond quickly and effectively, without taking sides.

facebook.com/icrc
twitter.com/icrc
instagram.com/icrc

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org

4403/002 10.2019 500