International Review of the Red Cross (2020), **102** (913), 1–22.
Digital technologies and war
doi:10.1017/S1816383121000114

IRRC

EDITORIAL

THE ROLE OF DIGITAL TECHNOLOGIES IN HUMANITARIAN LAW, POLICY AND ACTION: CHARTING A PATH FORWARD

Saman Rejali and Yannick Heiniger*

Why does "Digital Technologies and War" deserve the thematic focus of an entire issue of the *International Review of the Red Cross*? Contributors to this issue highlight two overarching reasons.

First, digitalization is a priority topic for humanitarian organizations like the International Committee of the Red Cross (ICRC)[1] because it is rapidly shaping how humanitarian operations and assistance activities are carried out, impacting how the humanitarian sector is serving affected populations.

In this respect, one group of contributors to this issue (with their pieces appearing under the headers "Humanitarian Action in the Digital Age" and "Business and Digital Technologies in Humanitarian Crises") analyze how the use of digital technologies for delivering humanitarian relief brings forth both unparalleled opportunities and risks. They highlight that some digital technologies, including those which ease communication and service delivery, are vital tools for the humanitarian sector. Those technologies help to ensure that the humanitarian sector brings solutions to crisis contexts and continues to serve affected populations. For example, increased connectivity and digital access can empower affected people in armed conflicts and other situations of violence to connect with others via messaging applications and social media platforms, to find information online and to express their needs via rapid feedback mechanisms, serving as active agents working with humanitarians.[2] Furthermore, digitally rooted contextual analyses, crisis mapping, and digitalized services can allow humanitarians to more efficiently serve affected people, and to predict and respond to humanitarian crises.

On the other hand, these contributors also stress how there are certain risks and considerations that go hand in hand with the opportunities brought forth in using digital technologies for humanitarian relief efforts. Accounting for and mitigating these risks is how the humanitarian sector can ensure that it is well prepared as it embarks on digital transformation processes. One dominant risk factor is data protection and privacy: collecting data from affected populations

* Saman Rejali is a Law and Policy Adviser at the ICRC and was Thematic Editor at the ICRC for this issue of the *Review* on "Digital Technologies and War". Yannick Heiniger is Deputy CEO of Swissnex San Francisco and was previously Partnerships Manager within the Office of the Director for Digital Transformation and Data at the ICRC.

puts an undeniable onus on humanitarian organizations to ensure that affected people's data is not misused and does not put them in harm's way, contrary to the purpose for which it was collected. Moreover, the ways in which data and information are disseminated are shaping how conflicts and other situations of violence unfold, in contexts such as Myanmar.[3] Misinformation, disinformation and hate speech (MDH), and the "new realities" presented through deepfakes (using machine learning to generate synthetic video, audio and text content),[4] are among the new risks that have come together with the widespread use of social media platforms and other online dissemination tools. As such, one section of this issue is dedicated to the role of businesses – more specifically, technology companies, which have been increasingly involved in supporting the work of humanitarian organizations, while concurrently being indirectly involved in the conduct of hostilities through the way their technologies are used.

There is also a second reason why digitalization matters for the humanitarian sector. Digital technologies (or "new" technologies) are used in armed conflicts as a means and method of warfare, governed by international humanitarian law (IHL). The uses of these new technologies have humanitarian consequences as they are giving rise to unprecedented means and methods of warfare. For example, as Gisel, Rodenhäuser and Dörmann point out in their article for this issue, cyber operations against electricity grids, health-care systems, nuclear facilities or other critical infrastructure could cause "significant human harm", with catastrophic humanitarian consequences.[5] Besides cyber threats, autonomous weapon systems (AWSs), including those enabled by artificial intelligence (AI), also raise humanitarian, legal and ethical concerns, as they select and apply force to targets without human intervention, meaning that the user does not know the specific target that will be struck, nor where or when.[6] In the third and fourth parts of this issue – focusing on AI and AWSs, and cyber operations and warfare, respectively – the contributors take different stances and

1 In the case of ICRC, "Embracing the Digital Transformation" is the fifth pillar of the organization's Institutional Strategy for 2019–22, available at: www.icrc.org/en/publication/4354-icrc-strategy-2019-2022 (all internet references were accessed in January 2021).

2 A look at the cover of this issue reflects this reality: in Syria, where emergency and long-term needs are great following years of violence, a father holds a smartphone in his hand, a photo of his son displayed on-screen, surrounded by the destruction created by the armed conflict. See "In Eastern Ghouta Rubble, a Father Looks for His Son", *Reuters*, 4 March 2018, available at: www.reuters.com/article/us-mideast-crisis-syria-ghouta-victims-idUSKBN1GG0EJ.

3 Alexandra Stevenson, "Facebook Admits It Was Used to Incite Violence in Myanmar", *New York Times*, 6 November 2018, available at: www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

4 Aengus Collins, *Forged Authenticity: Governing Deepfake Risks*, EPFL International Risk Governance Center, 2019, available at: https://infoscience.epfl.ch/record/273296?ln=en.

5 See Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts", in this issue of the *Review*.

6 See Vincent Boulanin, Neil Davison, Netta Goussac and Moa Peldán Carlsson, *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*, SIPRI and ICRC, June 2020, covered in the "Reports and Documents" section of this issue of the *Review*; Frank Sauer, "Stepping Back from the Brink: Why Regulating Autonomy in Weapons Systems is Difficult, Yet Imperative and Feasible", in this issue of the *Review*.

offer varying perspectives exploring how digital technologies are used in warfare, assessing the application of IHL to cases where digital technologies are used for destructive purposes.

"New" technologies, however, are ever evolving with the latest advancements. Just as the telegraph – now all but gone – was a "communication game changer"[7] two centuries back, some of the current "new" technologies will one day no longer be relevant, let alone "new", and perhaps the risks and opportunities relating to data protection and MDH will be moot. However, there are a series of "timeless" themes relating to digital technologies and humanitarian law, policy and action, which will stand the test of time, and are highlighted in the discussion that follows.

We[8] believe that one key common thread across these contributions is that of trust: principled humanitarian action is rooted in trust, and humanitarians have a responsibility to gain the trust of the affected populations they aim to serve.[9] While digital technologies offer unparalleled opportunities for providing humanitarian relief, they must be used ethically and responsibly in order to minimize the risks outlined in these pages. It is only by so doing that humanitarians can hope to gain the trust of the affected populations to whom they are accountable.

Along with trust comes ethics: operating in a way that does justice to the people we serve, ensuring that the benefits derived from digital technologies outweigh their risks, and ensuring that we work *with* affected people and do not decide for them on the issues that shape their lives. Ethical frameworks also apply to the means and methods of warfare. For example, when it comes to the uses of AI, Pizzi, Romanoff and Engelhardt[10] of UN Pulse, the UN Secretary-General's initiative on big data and AI, point to how ethical frameworks are necessary when regulating AI, but are not always sufficient in organizational structures where an "ethics-first approach" often does not go hand in hand with robust accountability mechanisms.

The authors featured in this issue also highlight the ethical considerations and potential inclusivity barriers to "humanitarian innovation". Humanitarian innovation has the possibility to open up new ways for us to serve affected people, but if innovative projects don't take into account data and personal information protection measures, and if they're created without truly being centred around and inclusive of affected people, then the risks they pose may outweigh the benefits.[11] In such cases, the "product" can outpace the due

7 Jimmy Stamp, "How the Telegraph Went from Semaphore to Communication Game Changer", *Smithsonian Magazine*, 11 October 2013, available at: www.smithsonianmag.com/arts-culture/how-the-telegraph-went-from-semaphore-to-communication-game-changer-1403433/.

8 The term "we" in this paper refers solely to the authors of this editorial and not to the ICRC or the humanitarian sector. The views expressed in this editorial reflect solely those of the authors and not those of the ICRC nor Swissnex San Francisco.

9 Hugo Slim, "Trust Me – I'm a Humanitarian", *Humanitarian Law and Policy Blog*, 24 October 2019, available at: https://blogs.icrc.org/law-and-policy/2019/10/24/trust-humanitarian/.

10 See Michael Pizzi, Mila Romanoff and Tim Engelhardt, "AI for Humanitarian Action: Human Rights and Ethics", appearing in this issue of the *Review*.

11 See ICRC, *Symposium Report: Digital Risks in Armed Conflicts*, Geneva, October 2019, covered in the "Reports and Documents" section of this issue of the *Review*.

diligence required to ensure that digital technologies cause more benefit than harm to affected populations. Indeed, this is a point echoed by Sandvik and Lohne,[12] who clearly identify that the problem is that "affected populations are often not present in innovation processes – they are neither properly consulted nor invited to participate". This potentially produces "new digital harms, whether these occur through (in)visibilizing the suffering of particular groups or individuals, creating undesirable consequences, or introducing new risks".

In what follows, we will first highlight how the contributions in this issue explore the benefits and risks of digital technologies used for humanitarian action, identifying the opportunities and mitigating measures to be taken as paths forward if we want to embark on a digitalization of humanitarian action, taking into account the growing role of the private sector. Thereafter, we will provide an overview of how digital technologies can be used as a means and method of warfare in armed conflict, making reference to contributions that explore themes of cyber operations and the application of IHL, as well as AWSs, machine learning and AI. This analysis is framed by outlining who we are, as two millennials with expertise on the theme at hand co-authoring this editorial, and concludes by addressing some contextual elements that impacted the publication of this issue of the *Review* and reflecting on the overall takeaway from the issue.

Millennial views on digital technologies and war

With this editorial, our purpose is to offer a cross-cutting glimpse into the diverse ideas that you will encounter throughout this issue of the *Review*. As two millennials who have been working on the broad theme of technologies in humanitarian action for a few years, we are admittedly part of the first generation of "digital natives".[13] We are supposed to be at ease with using and integrating new digital technologies into our daily lives. This is surely true when it comes to many aspects of our social lives: Facebook, Twitter, LinkedIn, TikTok and the likes are consuming a significant amount of our time, and digital interactions are perceived by many as an essential complement to physical ones.

As the ICRC's 2020 *Millennials on War* report highlights,[14] the perspective of millennials on the potential for digital technologies to help the people affected by war is quite positive. By exploring the impact and implications of digital technologies in armed conflicts and other situations of violence, our desire is that this issue of the *Review* will provide a "reality check" into the world that we, as millennials, are contributing to creating, highlighting how our actions in the

12 See Kristin Bergtora Sandvik and Kjersti Lohne, "The Struggle against Sexual Violence in Conflict: Investigating the Digital Turn", in this issue of the *Review*.

13 Berkman Klein Center for Internet and Society at Harvard University (BKC), "Digital Natives", available at: https://cyber.harvard.edu/research/youthandmedia/digitalnatives. Digital natives are defined by the BKC as "a generation 'born digital' – those who grow up immersed in digital technologies, for whom a life fully integrated with digital devices is the norm".

14 ICRC, *Millennials on War*, Geneva, 2020, available at: www.icrc.org/en/millennials-on-war.

humanitarian sphere have consequences for the affected people whom we aim to serve. We also recognize that we have our own biases as millennials. "Digital natives" tend to have a different relationship with the principles that are at the core of humanitarian practice – neutrality, impartiality, and independence in humanitarian action (NIIHA).[15] Digital technologies and algorithms are playing an important role in how we view the world.

When it comes to the principle of humanity, we not only recognize that "suffering is universal and requires a response"[16] – we also take an "activist" stance. We use the various social media channels at our disposal to galvanize action, both online and offline.[17] We are writing as two co-authors who have grown up mainly in the global North, and we recognize that our experiences are not universal to all millennials but are rather those of a subset of "global citizens" in the hubs of Geneva, London, New York, Toronto and Paris (among others).[18] Our commitment to making a difference and not being *indifferent* to suffering means that we have stuck it out through a financial crisis (and a second one at the time of writing); we have carried out internship after internship, one short-term contract after another, foregoing the stable lives of our parents[19] for the global lives we lead,[20] in order to land on our feet and pursue our vocation in the humanitarian sector. We are not easily deterred, which is what the world needs, as we are grappling with the risks that digital technologies can pose for humanitarian action and how they can be misused in warfare. Our world is not exclusively State-driven – it is multipolar, with "an ever-increasing number" of non-State armed groups,[21] using digital technologies as a means of advancing their aims in armed conflicts.[22] Moreover, we've grown up with social media, but

15 In comparison, the Fundamental Principles of the International Red Cross and Red Crescent Movement (the Movement) include seven principles: humanity, impartiality, neutrality, independence, voluntary service, unity and universality. Jérémie Labbé and Pascal Daudin, "Applying the Humanitarian Principles : Reflecting on the Experience of the International Committee of the Red Cross", *International Review of the Red Cross*, Vol. 97, No. 897/898, 2016; Office of the UN High Commissioner for Refugees, "Humanitarian Principles", available at: https://emergency.unhcr.org/entry/44765/humanitarian-principles; ICRC, "The Fundamental Principles of the Red Cross and Red Crescent Movement", August 2015, available at: www.icrc.org/sites/default/files/topic/file_plus_list/4046-the_fundamental_principles_of_the_international_red_cross_and_red_crescent_movement.pdf.

16 ICRC, above note 15.

17 Emily Logan, "Millennial Activism: Tapping into a Network of Millennial Donors", available at: https://csic.georgetown.edu/magazine/millennial-activism-tapping-network-millennial-donors/.

18 April Rinne, "What Is Global Citizenship?", 9 November 2017, available at: www.weforum.org/agenda/2017/11/what-is-global-citizenship/.

19 Janet Adamy, "Millennials Slammed by Second Financial Crisis Fall Even Further Behind", *Wall Street Journal*, 9 August 2020, available at: www.wsj.com/articles/millennials-covid-financial-crisis-fall-behind-jobless-11596811470.

20 BKC, above note 13.

21 Jelena Nikolic, Tristan Ferraro and Thomas de Saint Maurice, "Aggregated Intensity: Classifying Coalitions of Non-State Armed Groups", *Humanitarian Law and Policy Blog*, 7 October 2020, available at: https://blogs.icrc.org/law-and-policy/2020/10/07/aggregated-intensity-classifying-coalitions-non-state-armed-groups/.

22 Delphine van Solinge, "Digital Risks for Populations in Armed Conflict: Five Key Gaps the Humanitarian Sector should Address", *Humanitarian Law and Policy Blog*, 12 June 2019, available at: https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/.

have increasingly grown critical of it as well.[23] This is particularly the case when looking specifically at global technology companies, and at how the recent coronavirus crisis has strengthened their hold on key aspects of our society, exacerbating the daily realities of many, including in humanitarian contexts.

As millennials, we advocate for an understanding of the principle of impartiality as being arguably the driving force towards genuine inclusion and diversity in the humanitarian sector.[24] As such, we are cognisant that while digital technologies can allow us to more easily connect with and reach out to affected people, they can also cause a digital divide, resulting in intersectional inequities in access to digital technologies and their associated benefits, and thereby putting certain affected populations at a disadvantage.[25] This digital divide is highlighted cogently by Jo Burton in her article for this issue of the *Review*, through the example of the digitalization of cash. As she notes,

> the increase in digital payments may deepen the "digital divide" …. Any person can use cash if they can get their hands on it, and providing the goods and services they need to pay for are available. … However, to use digital payments, the recipient will require a level of digital and financial literacy. It is estimated that only one in three adults globally shows an understanding of basic financial concepts, and that there are lower standards of financial literacy amongst women and the poor.[26]

As Burton's analysis highlights, intersectional inequity – including financial and gender-based inequity – deepens the digital divide. However, we believe that if we take action that embodies the impartiality principle, we can address the systemic inequities that hinder humanitarian response.

With regard to the neutrality principle, as millennials we have come to realize, through our first-hand experience with many a misinformation and disinformation campaign on social media, that because of the way certain people make use of digital technologies, such technologies are not necessarily neutral. This is clearly illustrated by the use of digital technologies for destructive means during armed conflicts and other situations of violence.

Altogether, our millennial views on NIIHA shape how we view, analyze and work with digital technologies in humanitarian crises and in the context of

23 Nick Statt, "Facebook's US User Base Declined by 15 Million since 2017, According to Survey", *The Verge*, 6 March 2019, available at: www.theverge.com/2019/3/6/18253274/facebook-users-decline-15-million-people-united-states-privacy-scandals; Jack Nicas, Mike Isaac and Sheera Frenkel, "Millions Flock to Telegram and Signal as Fears Grow over Big Tech", *New York Times*, 13 January 2021, available at: www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html.

24 Saman Rejali, "Race, Equity, and Neo-Colonial Legacies: Identifying Paths Forward for Principled Humanitarian Action", *Humanitarian Law and Policy Blog*, 16 July 2020, available at: https://blogs.icrc.org/law-and-policy/2020/07/16/race-equity-neo-colonial-legacies-humanitarian/.

25 Barnaby Willitts-King, John Bryant and Kerrie Holloway, *The Humanitarian "Digital Divide"*, Humanitarian Policy Group Working Paper, Overseas Development Institute, London, November 2019, p. 15; Lina Gurung, "The Digital Divide: An Inquiry from Feminist Perspectives", *Dhaulagiri Journal of Sociology and Anthropology*, Vol. 12, 2018.

26 See Jo Burton, "'Doing No Harm' in the Digital Age: What the Digitalization of Cash Means for Humanitarian Action", in this issue of the *Review*.

evaluating the application of IHL to the means and methods of warfare. The outlook on digital technologies provided in these pages gave us a unique opportunity to (re) think about and broaden our reflections on digital technologies and war, and the broader purpose that digital technologies serve for humanitarian action. We hope this will be the case for every reader, beyond generational boundaries.

Digital technologies and humanitarian action: The risks

A collection of the contributions in this issue highlight how digital technologies can be used without full awareness of what they will trigger. Thus, digital technologies pose certain risks within conflicts – societal, economic, political and cognitive – which must be accounted for in humanitarian assistance and operational activities. The most problematic issue, perhaps, is that benefit/risk assessments are often carried out solely by humanitarians, and not *with* affected people. Furthermore, those most affected by such risks are individuals and communities in crisis contexts.

There are three main vectors for risk[27] identified with respect to humanitarian action: (1) digital surveillance, monitoring and intrusion; (2) MDH; and (3) the misuse and mishandling of data and personal information.

Digital surveillance, monitoring and intrusion

The risks associated with digital surveillance, monitoring and intrusion can come from various sources, including big data analyses, machine learning models, misuse of data by authorities, and as a consequence of people's online presence and activities. As Gazi and Gazis[28] point out in their contribution to this issue, big data and open data analyses not only entail privacy risks but may also produce biased results. The latter is due to the fact that big data and open data

> often lack demographic information that is crucial for epidemiological research, such as age and sex. [Also], this data represents only a limited portion of the population – i.e., excluding marginalized and under-represented groups such as infants, illiterate persons, the elderly, indigenous communities and people with disabilities – while potentially under-representing some developing countries where digital access is not widespread.

This is particularly problematic for humanitarian assistance and protection activities, since big data and open data analytics can lead humanitarians to inadvertently ignore the marginalized people, standing at several intersections of

27 According to the ICRC's *Digital Risks in Armed Conflicts* Symposium Report, digital risks "include (often unintended) side-effects of digital data experimentation, privacy violations, and the mishandling of sensitive information that accompanies the humanitarian sector's efforts to deploy emerging technologies in already fragile contexts". ICRC, above note 11.

28 See Theodora Gazi and Alexandros Gazis, "Humanitarian Aid in the Age of COVID-19: A Review of Big Data Crisis Analytics and the General Data Protection Regulation", in this issue of the *Review*.

inequity, whom they aim to serve. This is reaffirmed by Milaninia[29] in his analysis, which illustrates how machine learning models and big data analytics are "highly susceptible to common human biases" and can thereby "accelerate existing racial, political or gender inequalities" and potentially paint "a misleading and distorted picture of the facts on the ground".

Similarly, Pizzi, Romanoff and Engelhardt[30] illustrate that a lack of quality data increases the risks that an AI system will produce unfair outcomes, as

> AI systems can reveal sensitive insights into individuals' whereabouts, social networks, political affiliations, sexual preferences and more, all based on data that people voluntarily post online (such as the text and photos that users post to social media) or incidentally produce from their digital devices (such as GPS or cell-site location data).

Once this data is collected, it is highly susceptible to misuse, if necessary data protection measures are not taken. Most dangerously, through their online behaviour, affected populations can unknowingly be subjecting themselves to potential offline harm, including but not limited to being surveilled and profiled in crisis contexts,[31] and facing the threat of violence, hate crimes and/or discrimination.[32] A real case scenario of such surveillance is provided in the ICRC's Symposium Report on *Digital Risks in Armed Conflicts*, featured in the "Reports and Documents" section of this issue, whereby Syrian refugees' mobile devices were compromised through a malware attack. Other examples show surveillance occurring by humanitarians themselves as they use technologies to better respond to needs – for example, via drone usage for mapping and risk assessment purposes.[33] Here, the aforementioned risks of surveillance particularly apply as the drones may gather information from contexts where affected populations live, without their consent and/or knowledge. More sophisticated illustrations of surveillance, monitoring and intrusion can be found, for instance, in the article by Siatitsa,[34] which discusses such issues in relation to facial recognition.

Misinformation, disinformation and hate speech

Speaking about MDH in the Q&A conducted for this issue of the *Review*,[35] Delphine van Solinge unpacks how through MDH, information can be manipulated and

29 See Nema Milaninia, "Biases in Machine Learning Models and Big Data Analytics: The International Criminal and Humanitarian Law Implications", in this issue of the *Review*.
30 M. Pizzi, M. Romanoff and T. Engelhardt, above note 10.
31 J. Burton, above note 26.
32 ICRC, above note 11.
33 Faine Greenwood, "Data Colonialism, Surveillance Capitalism and Drones", in Doug Specht (ed.), *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, University of London Press, London, 2020.
34 See Ilia Siatitsa, "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications", in this issue of the *Review*.
35 See "Q&A: Humanitarian Operations, the Spread of Harmful Information and Data Protection", in this issue of the *Review*.

spread using digital technologies – particularly amidst the coronavirus pandemic, when populations are more reliant on digital communication technologies. An example of a disinformation tactic is the creation of "deepfakes", using machine learning to generate fake video and audio content.[36] In crisis contexts such as Myanmar, South Sudan and Ethiopia,[37] MDH are disseminated via social media platforms, and public opinion is manipulated based on false or incomplete information, exacerbating the humanitarian crises at hand. The use of technologies by mass publics gives increasing power to the companies behind social media, messaging and search platforms, including in armed conflicts and other situations of violence. We have seen recently how big technology firms have had reverberating global effects in being arbiters between freedom of speech, on the one hand, and social media accounts being used for the spreading of harmful information (i.e., MDH), on the other. This is more the case now, during the coronavirus pandemic, as affected populations are more reliant than ever before on such platforms to receive information and communicate with each other.

The misuse and mishandling of data and personal information

When it comes to the misuse and mishandling of data, the concept of "technocolonialism", coined by Mirca Madianou,[38] serves as an excellent guiding light for what can go wrong, even with the best of intentions, if we strive for digital innovation and aggregate biometric data in humanitarian crises without putting in place the necessary data protection practices and digitally tailored protection frameworks. Indeed, technologies integrate and reinforce the value systems, cultures and world views of their builders. Uninhibited digital innovation and data practices can further ingrain the colonially rooted power asymmetries between humanitarian actors and affected populations.[39]

This is reflected in the occurrence of "surveillance capitalism", described by Zuboff as "data from humans used to turn a profit, at the expense of the people themselves".[40] In the context of humanitarian crises, this means that data from affected populations can be not only collected but also used for profit. As this collection of data often happens without the knowledge of the affected person, Zuboff draws a parallel with colonial practices of extraction without permission. In this respect, Sandvik and Lohne note how the ramifications of such uninhibited gathering of data, and the recording of affected populations'

36 Harvard Kennedy School, Belfer Centre for Science and Information Affairs, "Tech Factsheets for Policymakers: Deepfakes", Spring 2020, available at: www.belfercenter.org/sites/default/files/2020-10/tappfactsheets/Deepfakes.pdf.
37 "Q&A", above note 35.
38 Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", *Social Media + Society*, Vol. 5, No. 3, 2019, available at: https://journals.sagepub.com/doi/full/10.1177/2056305119863146.
39 *Ibid.*
40 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future*, PublicAffairs, New York, 2019.

information on digital clouds, can create "digital bodies" with gendered ramifications for how we address conflict-related sexual violence.[41]

The after-effects of what happens in the humanitarian sector when data protection measures are not implemented properly are highlighted by Massimo Marelli in this issue's Q&A,[42] and by Burton, who applies the "do no (digital) harm" principle of data protection to the digitalization of cash. Burton highlights how metadata – data that provides information about other data – can have grave consequences for humanitarian crises and can be used for military gain, particularly when we hear influential people such as General Hayden, former director of the US National Security Agency and Central Intelligence Agency, quoted by Burton, saying: "We kill people based on metadata."[43]

The issue of what happens to affected populations' data once collected by humanitarian organizations is critical. Large technology companies have on several occasions shared users' data with governments, which can pose security risks to citizens living in armed conflicts or other situations of violence.[44] It is worth noting that even when affected people's data is not shared, the stored data may be hacked into or stolen if not well protected by humanitarian organizations.[45] This data protection risk is highlighted in the ICRC's Symposium Report[46] as well: "Humanitarian organizations collect, store, share, and analyze data that is attractive to parties to armed conflict. … As a result, humanitarian organizations are exposed to a growing wave of digital attacks and cyber espionage, and have become highly prized targets."

Digital technologies and humanitarian action: Mitigating measures and benefits

To account for these digital risks, which have societal, economic, political and cognitive consequences for affected populations and humanitarian crises, there are several active steps that can be taken, including (1) fostering digital literacy, (2) strengthening data protection practices and creating the right safeguards for the adoption of digital technologies, and (3) adopting suitable humanitarian policies, ensuring humanitarians continue to put people at the centre of their work.

Fostering digital literacy

Digital literacy is not just a "nice to have" component for humanitarian organizations; it is a crucial necessity for affected populations. This important observation emerges

41 K. B. Sandvik and K. Lohne, above note 12.
42 "Q&A", above note 35.
43 J. Burton, above note 26.
44 *Ibid.*; F. Greenwood, above note 33.
45 The importance of data protection measures in humanitarian action is highlighted in Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, 2nd ed., ICRC and Brussels Privacy Hub, Geneva, June 2020, covered in the "Reports and Documents" section of this issue of the *Review*.
46 ICRC, above note 11.

several times throughout this issue of the *Review*. Van Solinge, for instance, advocates for increasing people's resilience to misinformation and disinformation by "promoting digital literacy, critical thinking and … humanitarian values".[47] Sandvik and Lohne, for their part, highlight how digital literacy must go "beyond technical competence to include awareness and perceptions about technology, law, rights and risk".[48] These elements are also crucial for humanitarian organizations themselves. As an example of ongoing initiatives aimed at giving humanitarian decision-makers and lawyers crucial digital literacy skills, the ICRC has now partnered with the Swiss Federal Institute of Technology Lausanne (Ecole Polytechnique Fédérale de Lausanne, EPFL) on a series of collaborative initiatives,[49] including one to create a five-day introductory course on information and communication technology fundamentals.[50] Along the same lines, the International Federation of Red Cross and Red Crescent Societies (IFRC) has developed a Data Playbook Project, aiming to "improve data literacy across teams, sectors, the IFRC Secretariat, and within National Societies".[51] While these concrete projects focus on humanitarian actors themselves, they are a first step into a new territory for many humanitarian organizations, and call for similar initiatives at the field level focusing on affected populations and their digital literacy.

Strengthening data protection practices

Alongside digital literacy skills, appropriate data protection practices can ensure that unwanted access to affected populations' data – through surveillance, monitoring or breach of digital storage solutions – is prevented, serving as another mitigating measure for digital risk. In this respect, for example, Massimo Marelli highlights how the ICRC has

> now adopted several specific safeguards in [its] Rules on Personal Data Protection, adopted in 2015, which are designed to reduce the risk of unauthorized use or access to personal data by applying data protection standards and requirements to data processing throughout the organization. Where new technologies or riskier data processing operations are considered by the ICRC, a Data Protection Impact Assessment must be conducted to identify and mitigate the risks of harm. The Rules also require the ICRC to follow a "data protection by design" approach to minimize the collection of

47 "Q&A", above note 35.
48 K. B. Sandvik and K. Lohne, above note 12.
49 The EPFL and ETH Zürich are joining forces with the ICRC to explore innovative solutions to today's humanitarian crises, through the HAC initiative: see EPFL, "Science and Technology for Humanitarian Action Challenges (HAC)", available at: www.epfl.ch/research/services/fund-research/funding-opportunities/research-funding/science-and-technology-for-humanitarian-action-challenges-hac/. See also EPFL, "EPFL, ETH Zurich and the ICRC Team Up to Bolster Humanitarian Aid", 10 December 2020, available at: https://actu.epfl.ch/news/epfl-eth-zurich-and-the-icrc-team-up-to-bolster-hu/.
50 EPFL, "Executive Training: Foundations of Information and Communication Technologies", available at: www.c4dt.org/event/fict-executive-course/.
51 IFRC, "Discover the Data Playbook Beta Project", 18 October 2018, available at: https://media.ifrc.org/ifrc/2018/10/18/discover-data-playbook-beta-project/.

personal data to that which is necessary for the operation and ensure that data subjects' rights are respected.[52]

Humanitarian policy as an enabler for the responsible use of technologies

Among the resources available to humanitarians in this process of balancing opportunities and risks, policy emerges as a unique enabler. As we look for organizations engaging in digital transformation processes while ensuring that digital risks are mitigated, a few interesting examples come to mind, which complement what you will find in this issue of the *Review*. One of the key resolutions of the 33rd International Conference of the Red Cross and Red Crescent (International Conference) in 2019 was Resolution 4 on "Restoring Family Links while Respecting Privacy, Including as it Relates to Personal Data Protection".[53] This resolution calls on States and the International Red Cross and Red Crescent Movement (the Movement) to respect numerous privacy and data protection stipulations when processing the information of affected populations. In particular, it "urges States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement."[54] The data protection stipulations that underpin this resolution are embodied within the *Restoring Family Links Code of Conduct on Data Protection*.[55] This code of conduct sets out the minimum principles, commitments and procedures that personnel of the ICRC, National Societies and the IFRC must comply with when processing personal data within the framework of Restoring Family Links activities. Such documents can ensure that humanitarians have a common understanding of the inherent risks and common measures needed to make sure technologies work in a way that reinforces the protection of the sensitive data of individuals in conflict zones.

In fact, the 2019 International Conference also yielded a Movement-wide Digital Pledge on "Strengthening National Digital and Data Capacities for Humanitarian Action",[56] whereby the Movement committed to an action plan by the end of 2023 to (1) foster partnerships in this respect; (2) convene regarding these issues; and commit to (3) digital literacy, (4) digital inclusion, (5) data protection and (6) digital responsibility. This example is another illustration of the importance of embracing a principled digital transformation journey and aligning visions around the measures needed to mitigate the adverse effects of

52 "Q&A", above note 35.

53 ICRC, "Restoring Family Links while Respecting Privacy, Including as it Relates to Personal Data Protection", 33IC/19/R4, Resolution 4 adopted at the 33rd International Conference of the Red Cross and Red Crescent, Geneva, 9–12 December 2019, available at: https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

54 *Ibid.*, para. 11.

55 ICRC, *Restoring Family Links Code of Conduct on Data Protection*, Geneva, November 2015, available at: www.icrc.org/en/document/rfl-code-conduct.

56 "Strengthening National Digital and Data Capacities for Humanitarian Action", Digital Pledge, 2019 International Conference, available at: https://tinyurl.com/110x3pmp.

digital technologies. It also shows how the Movement can lead by example in translating the Movement-wide Fundamental Principles[57] to the use of such technologies.

Still in the domain of humanitarian policy, in 2019 the ICRC also produced a policy stance on its use of biometric technologies,[58] which are used in forensics and the restoration of family links. Given the sensitivity of creating a permanent record for individuals who may not want to be identifiable forever, this policy facilitates a responsible use of the technology by the organization and addresses the data protection challenges this poses. Overall, these multiple initiatives illustrate well the role that humanitarian policy can play in creating an actionable framework enabling the principled use of new digital technologies.

Benefits of digital technologies for humanitarian action

While digital technologies pose certain aforementioned risks, they also bring unparalleled benefits for how humanitarian operational and assistance activities are carried out. This is exemplified in this issue of the *Review* through the "Voices and Perspectives" section, which features testimonies collected from affected populations.

This section presents direct quotes from individuals whose lives have changed for the better because of the digitally driven initiatives heralded by the ICRC. One testimony focuses on the ICRC's Trace the Face platform,[59] which is an "online photo gallery with thousands of pictures of people looking for their family." It was through this site that Matty, based in Abidjan, was able to find his uncle, whom he'd had no news of since the outbreak of the 2010–11 crisis in Ivory Coast.[60]

Similarly highlighting the positive potentials for digital technologies in humanitarian crises, the other featured testimony is from Zawadi, who talks about how she was able to connect with her husband's family through the Electronic Red Cross Messaging initiative, which is a collaborative pilot project between the ICRC, the Congolese Red Cross and the Rwandan Red Cross.[61] The pilot project began in November 2018 and uses digital Red Cross messages to re-establish links between separated family members. As a part of the project, Red Cross volunteers roam the villages of the eastern Democratic Republic of the Congo and Rwanda with digital tablets connected to the Internet. The project shows great promise as it has improved one of the oldest services at the ICRC, the Red Cross messaging system, managing to facilitate the work of restoring

57 ICRC, above note 15.
58 ICRC, "The ICRC Biometrics Policy", 16 October 2019, available at: www.icrc.org/en/document/icrc-biometrics-policy.
59 ICRC, "Trace the Face – Migrants in Europe", available at: https://familylinks.icrc.org/europe/en/pages/publish-your-photo.aspx.
60 See "How Humanitarian Technologies Impact the Lives of Affected Populations", in the "Voices and Perspectives" section of this issue of the *Review*.
61 *Ibid.*

links between families in a faster and more efficient manner than before. Such initiatives, as seen through the testimonies of affected people, serve as examples of what is possible when humanitarian innovation merges with digital technologies with the aim of alleviating human suffering in armed conflicts and other situations of violence. Building on this momentum, the ICRC is piloting Red Safe,[62] a digital platform allowing affected populations to access a variety of services digitally.

In her Q&A with the *Review*, Delphine van Solinge also highlights how humanitarian practitioners have "made use of the enhanced situational awareness and actionable information afforded by the digital age". For example, as she points out, human rights defenders and humanitarian practitioners have

> employed remote sensing tools for augmenting conflict early warning capacities and documenting human rights abuses. They have leveraged mobile data solutions for tracking the conditions, profiles and routes of transit of migrant and refugee populations; exploited metadata from call detail records to understand the spread of infectious diseases; harvested social media for sentiment analysis and rumour tracking in fragile contexts; and of course, they've deployed aerial robotics for surveillance of damaged locations and monitoring critical infrastructure.
>
> In the case of COVID-19, digital tools, artificial intelligence and "big data" analysis are being used in various contexts to support health-based responses. They can help us collect, analyze and transmit critical information in order to organize health resources and capabilities, accelerate medical logistical and procurement chains or manage the public safety and security dimensions of confinement.

While Gazi and Gazis[63] analyze the aforementioned risks of using big data in their contribution to this issue of the *Review*, they also highlight the potential benefits of big data for humanitarian action. They note how in the context of disaster management, big data can help with responding to migration crises, epidemics and natural disasters, as well as epidemic surveillance and response. A notable example they put forward is that of Ushahidi, a software application used to improve humanitarian relief efforts. Through using the platform, researchers in Kenya

> analyzed the geographic mobile phone records of nearly 15 million individuals between June 2008 and June 2009 in order to measure human mobility in low-income settings in Kenya and understand the spread of malaria and infectious diseases. The Kenyan phone company Safaricom provided de-identified information to researchers, who then modelled users' travel patterns. Researchers estimated the probability of residents and visitors being infected in each area by cross-checking their journeys with the malaria prevalence map provided by the government.

62 See ICRC, "ICRC'S Activities in Favour of Migrants in Southern Africa", 2020, p. 5, available at: www.icrc.org/en/download/file/147853/icrcs_activities_in_favour_of_migrants_in_southern_africa_newsletter.pdf.

63 T. Gazi and A. Gazis, above note 28.

The use of such data to track infectious diseases has great potential, especially during the current age of COVID-19. Granted, as Gazi and Gazis stress, any such harvesting of data poses "re-identification risks based on persons' unique activity patterns. For this reason, when de-identified personal data are used for analysis purposes, anonymization procedures typically alter the original data slightly (causing a loss of data utility) in order to protect individuals' identities".

Also highlighting some of the benefits of digital technologies for monitoring compliance with IHL, as well as for other purposes, Milaninia[64] discusses how machine learning is being used positively, "including to uncover mass graves in Mexico, find evidence of homes and schools destroyed in Darfur, detect fake videos and doctored evidence, predict the outcomes of judicial hearings at the European Court of Human Rights, and gather evidence of war crimes in Syria".

These contributors thus balance the benefits and risks of digital technologies for humanitarian action and beyond, noting how necessary it is that humanitarian practitioners make use of digital technologies while taking the appropriate mitigation measures.

Humanitarians engaging with the technology sector

Another interesting avenue emerging from this issue on digital technologies relates to the interactions between humanitarians and the actors who create these technologies. We have mentioned how technologies are used in cyber operations and their potential humanitarian consequences, a topic developed further in the "Cyber Operations and Warfare" section of this issue and covered in the next part of this editorial. Technologies are not developed in a vacuum – they are products and solutions developed by specific companies. In this context, how can humanitarian actors, who have built on decades of proven experience in "humanitarian diplomacy",[65] better interact with the technology sector? A few examples come to mind, illustrating both the substance of a possible dialogue and the forms it can take.

In this issue, Massimo Marelli highlights how specific digital infrastructures and solutions are needed to ensure that the organization remains in full control of the sensitive data it manages – for instance, through the creation of a digital humanitarian space along the model of a "sovereign cloud" or a "digital embassy".[66] The development of new technologies ensuring that the data collected by the ICRC under its mandate are and remain at all times under its exclusive control indicates one productive area for enhanced dialogue and

64 N. Milaninia, above note 29.

65 ICRC, "Humanitarian Diplomacy", available at: www.icrc.org/en/what-we-do/humanitarian-diplomacy-and-communication.

66 See Massimo Marelli, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation", in this issue of the *Review*.

concrete collaboration between humanitarians, the technology sector, governments and academics.[67]

In this regard, the ICRC has established a presence in the Bay Area of the United States as a step towards building a sustained dialogue with global tech companies on the way digital tools can impact people affected by armed conflicts and other situations of violence.[68] The main thrust of engagement is bringing the ICRC's operational and legal expertise, and its contextual knowledge, to a dialogue centred on the drive to ensure responsible use of technologies – which includes the core principles of privacy and trust – in humanitarian settings. This requires mutual learning about how technology may, on the one hand, be of help to populations in conflict zones, and, on the other, create different risks and harms for these individuals, communities and societies. On that basis, efforts are being made to ensure that the technology that the ICRC uses, and that affected populations use (and are exposed to), is as effective and safe as possible. This may entail the co-creation of new tools and services (such as those previously mentioned that are not easily available "off the shelf" from commercial suppliers), as well as humanitarian diplomacy to convince different stakeholders to support the ICRC, its approach and its (legal, policy and/or ethical) recommendations.

At the same time, a privileged dialogue with the technology sector is also key to better understanding its intellectual bedrock. At the heart of the growing interest from technology firms towards collaboration with humanitarians is the conviction not only that digital technologies are a source of good, but also that they can help humanitarian actors to meet the needs of affected populations efficiently and with lasting positive effects. Nevertheless, the interaction can easily be marred by "technological determinism"[69] and a "hero-preneuership culture".[70] It has been argued that these two concepts are closely connected to the Bay Area of the United States,[71] where two widespread beliefs are that technology is "leading to good outcomes for everyone" and that "new kinds of technologies should be deployed as quickly as possible, even if we lack a general idea of how the technology works, or what the societal impact will be".[72] This is one of the dimensions at play when Jo Burton, quoting Nathaniel Raymond, encourages humanitarians to avoid a "blind embrace of the potential 'promises of Silicon

67 EPFL, "EPFL, ETH Zurich and the ICRC Leverage Science and Technology to Address Humanitarian Challenges", 10 December 2020, available at: https://essentialtech.center/engineering-humanitarian-aid-awards-six-epfl-ethz-icrc-projects/.

68 Sean Capitain, "The Red Cross Presses Silicon Valley to Fight Cyberwarfare", *Fast Company*, 10 October 2017, available at: https://www.fastcompany.com/40476581/red-cross-could-silicon-valley-limit-cyberwarfare-if-governments-wont.

69 John Naughton "Think the Giants of Silicon Valley Have Your Best Interests at Heart? Think Again", *The Guardian*, 21 October 2018, available at: www.theguardian.com/commentisfree/2018/oct/21/think-the-giants-of-silicon-valley-have-your-best-interestsat-heart-think-again.

70 Daniela Papi-Thornton, "Tackling Heropreneurship", *Stanford Social Innovation Review*, 23 February 2016, available at: https://ssir.org/articles/entry/tackling_heropreneurship#.

71 Jasmine Sun, "Silicon Valley's Saviorism Problem", *The Stanford Daily*, 16 February 2018, available at: www.stanforddaily.com/2018/02/16/silicon-valleys-saviorism-problem/.

72 J. Naughton, above note 69.

Valley'", as its tendency to reduce complicated problems to a technological solution is surely at odds with the complexity faced in conflict zones. These assumptions can have massive implications when considering the adoption of technologies in humanitarian action and calls for a critical engagement with the technology sector and its companies and workforce, anywhere technology is developed.

The pilot nature of the engagement in the Bay Area illustrates the potential for similar dialogues in other hubs where digital technologies are being developed, potentially shaping future cyber operations. While the ICRC has recently strengthened its technology engagements in Japan,[73] there is surely room for similar interactions in other technology hubs around the world.

Multilateralism and the development of international law

The growing influence of the private sector also has implications on multilateralism and the development of law, a topic explored in more depth in this issue. Given the fast rise of the technology sector and the widespread use of digital technologies, Ambassador Amandeep S. Gill, in his contribution "The Changing Role of Multilateral Forums in Regulating Armed Conflict in the Digital Age",[74] identifies the structural issues that make it difficult for multilateral forums to discuss fast-moving digital issues and respond in time with required norms and policy measures. For Gill,

> [w]hile private companies and civil society have had an important agenda-setting and opinion-shaping role in some discussions, they take a secondary position to more powerful State and inter-State actors. This power asymmetry sits uneasily with the digital technology reality. For example, digital platforms such as Facebook, Alipay and WhatsApp may have more users ("virtual residents") than the populations of most countries; they operate quasi-global infrastructures, act as cross-border "content policemen" and have market capitalizations that dwarf other sectors and most national GDPs.

Gill's article highlights that "[i]f norms related to digital technologies are to have an impact, the digital industry has to be a part of the discussion on policy responses and has to cooperate with State-actors for their implementation".

Such a claim is also relevant for the humanitarian sector, particularly when it comes to IHL and its development. Given the complexities of how technologies work, how fast they evolve and the fact that their capabilities remain largely unknown, the international community and humanitarians must find new ways to ensure that new technologies used as means and methods of warfare are compliant with IHL.

73 NEC, "NEC and ICRC: A Blueprint for Ethical Technology Partnerships between the Private and Humanitarian Sectors", 11 November 2020, available at: www.nec.com/en/global/sdgs/innovators/project/article02.html.

74 See Amandeep S. Gill, "The Changing Role of Multilateral Forums in Regulating Armed Conflict in the Digital Age", in this issue of the *Review*.

Digital technologies and the means and methods of warfare

The second half of this issue of the *Review* shifts the focus from how digital technologies can be used for humanitarian relief, assessing the risks and benefits of their use, to how new technologies can used for destructive purposes in armed conflicts.

In this regard, Frank Sauer's contribution[75] engages with the implications of not regulating autonomous weapons systems, including those that rely on AI. Unpacking the costs of non-regulation, Sauer makes a robust case for why regulating AWSs is difficult, but nevertheless quite imperative on ethical, legal and policy grounds. As Sauer argues, it is essential that autonomy in weapons systems is regulated, by "codifying a legally binding obligation to retain meaningful human control over the use of force".

New applications of sensors and software, especially AI and machine-learning systems, also have broader implications for decision-making in armed conflict. Pizzi, Romanoff and Engelhardt argue that AI and machine learning "can be extremely powerful, generating analytical and predictive insights that increasingly outstrip human capabilities. They are therefore liable to be used as replacements for human decision-making, especially when analysis needs to be done rapidly or at scale, with human overseers often overlooking their risks and the potential for serious harms to individuals or groups of individuals that are already vulnerable."[76] The ICRC position paper "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach", updated for this issue of the *Review* and appearing in the "Reports and Documents" section, is more cautious, stressing that "AI and machine-learning systems remain tools that must be used to serve human actors, and augment human decision-makers, not replace them". It argues for an approach that foregrounds human legal and ethical obligations in order "to preserve human control and judgement in applications of AI and machine learning for tasks and in decisions that may have serious consequences for people's lives, especially where these tasks and decisions pose risks to life, and where they are governed by specific rules of international humanitarian law".[77] Both papers highlight the technical limitations of AI that bring legal questions; Pizzi, Romanoff and Engelhardt note how AI

> creates challenges for transparency and oversight, since designers and implementers are often unable to "peer into" AI systems and understand how and why a decision was made. This so-called "black box" problem can preclude effective accountability in cases where these systems cause harm, such as when an AI system makes or supports a decision that has discriminatory impact.[78]

75 F. Sauer, above note 6.
76 M. Pizzi, M. Romanoff and T. Engelhardt, above note 10.
77 See ICRC, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach", in this issue of the *Review*.
78 M. Pizzi, M. Romanoff and T. Engelhardt, above note 10.

New digital technologies are also set to influence cyber operations and cyber warfare. The adoption of new digital technologies by parties to an armed conflict has a direct effect on the means and methods of warfare itself, and consequently on the application and interpretation of IHL in that case. As Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann point out in their contribution to this issue:[79]

> [T]he use of cyber operations during armed conflict has become a reality of armed conflicts and is likely to be more prominent in the future. This development raises a number of concerns in today's ever more cyber-reliant societies, in which malicious cyber operations risk causing significant disruption and harm to humans. … The international community, societies, and each of us individually are increasingly relying on digital tools. This trend – which may be accelerated further by the COVID-19 pandemic spreading at the time of writing this article – increases our dependency on the uninterrupted functioning of these technologies, and thus increases our vulnerability to cyber operations.

The latter point is supported by recent findings by Freedom House,[80] which highlight how governments around the world have exploited the pandemic in order to expand their domestic surveillance capabilities, using, for instance, contact tracing apps that collect private information. Similarly, the CyberPeace Institute[81] has raised its voice regarding the growing and alarming number of cyber attacks. This phenomenon takes a particular shape when it comes to health-care infrastructures, because, as Gisel, Rodenhäuser and Dörmann point out, "The health-care sector seems particularly vulnerable to cyber attacks. The sector is moving towards increased digitization and interconnectivity, which increases its digital dependency and its attack surface."[82] These trends are also highlighted in the piece written by Zhixiong Huang and Yaohui Ying.[83] The authors cogently offer a different perspective on the application of the principle of distinction to the cyber context, by injecting the positions of Chinese officials and the views of Chinese scholars into the debate. They highlight how certain elements of distinction – such as uniforms and distinguishing marks – are either impractical or unworkable in the cyber sphere. While the principle of distinction remains relevant, the authors argue that it should be interpreted in a manner appropriate for the cyber realm.

79 L. Gisel, T. Rodenhäuser and K. Dörmann, above note 5.

80 Adrian Shahbaz and Allie Funk, "The Pandemic's Digital Shadow", Freedom House, 2020, available at: https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

81 CyberPeace Institute, "A Call to All Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector", 26 May 2020, available at: https://cyberpeaceinstitute.org/call-for-government/.

82 In light of this worrying trend, the ICRC has joined world leaders in calling to stop attacks against health-care infrastructure, particularly since these attacks could endanger the lives of vulnerable civilians. See "Call by Global Leaders: Work Together Now to Stop Cyberattacks on the Healthcare Sector", *Humanitarian Law and Policy Blog*, 26 May 2020, available at: https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/.

83 See Zhixiong Huang and Yaohui Ying, "The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective", in this issue of the *Review*.

Together, these contributions bring together not only diverse profiles of authors, but also diverse and multidisciplinary sets of analyses that enrich the ability of this issue of the *Review* to address how such digital technologies are, in times of armed conflict, regulated by IHL.

Thematic scope of this issue on "Digital Technologies and War"

As highlighted above, the contents of this issue of the *Review* touch on the dual uses for digital technologies: (1) for humanitarian action and relief – weighing the risks and benefits – aimed at assisting and protecting affected populations in armed conflicts and other situations of violence; and (2) for use in the conduct of warfare in armed conflicts. The contributions to this issue also account for the growing role of the private sector – especially big tech – in providing the platforms that are used for the dissemination of MDH and which shape how information is shared during crisis contexts.

In putting together this issue, the *Review* was cognisant that we are just beginning to unpack the patterns and trends in how digital technologies will affect the world. Thus, while this thematic issue on "Digital Technologies and War" opens up the black box to how digital technologies shape and are being shaped by armed conflicts and other situations of violence, it is not exhaustive. In other words, our current understanding of existing and emerging technologies is still increasing, bringing to light new challenges and opportunities around the digital technologies that we use, embrace, and at times, fear.

Gender, diversity and inclusion in the *Review*

An essential parameter for the production of this issue was gender parity and the inclusion of diverse profiles and views. Gender gaps in the technology sector are well known, with women comprising less than 35% of the workforce in the sector.[84] In terms of diversity, most of the largest technology companies[85] are populated by a near-homogenous group of young white males,[86] coming out of prestigious US universities,[87] with little or no training in humanities, ethics or

84 Sam Daley, "Women In Tech Statistics for 2020 (and How We Can Do Better)", *Built In*, 13 March 2020, available at: https://builtin.com/women-tech/women-in-tech-workplace-statistics.

85 Jonathan Ponciano, "The Largest Technology Companies in 2019: Apple Reigns as Smartphones Slip and Cloud Services Thrive", *Forbes*, 15 May 2019, available at: www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/.

86 Shelly Banjo and Dina Bass, "On Diversity, Silicon Valley Failed to Think Different", *Bloomberg Businessweek*, 3 August 2020, available at: www.bloomberg.com/news/articles/2020-08-03/silicon-valley-didn-t-inherit-discrimination-but-replicated-it-anyway.

87 Avery Hartmans, "These 25 Universities Produce the Most Tech Employees", *Business Insider*, 2 May 2017, available at: www.businessinsider.com/top-colleges-for-working-in-silicon-valley-2017-5.

international relations.[88] Moreover, it has been argued that there is gender and race discrimination evident in digital technologies themselves,[89] and in digital data, which carry structural biases, as they represent and amplify the societal discriminations and power relations that exist. The *Review* team's aim was to at least break with this trend in terms of the profiles of authors featured in this issue. Yet, we faced certain hurdles in this quest; as we were starting to produce this thematic issue during the late winter of 2019, the coronavirus hit us like no other pandemic in the last century.[90]

On the *Review*'s end, we witnessed the gendered effects of this crisis on our authorship composition. Numerous female authors whom we'd actively solicited dropped out of submitting their manuscripts to the journal. This is a trend that has been observed across the academic publishing sector: many female academics and authors have faced the double burden of housework and professional work at higher rates than their male counterparts. As more than a few of our female authors dropped out and female authors disproportionately turned down our invitations for submission to the journal, the *Review* prolonged its publication timeline to ensure that in the end, the final product was not dominated by one demographic. As our final selection evidences, while we unfortunately have not managed to reach perfect gender parity in authorship, the gender parity gap stands at 0.82 (female to male contributors) – a ratio that the *Review* is firmly and actively committed to closing with future issues.[91] Similarly, our quest for more diversity in our publications continues – most recently, for example, the *Review* has welcomed its new Editorial Board for the 2021–26 term, comprised of a diverse group of nineteen experts from around the world.[92]

The diversity element of the issue comes not just in the form of the backgrounds of the authors but is also enhanced by the cross-disciplinary and multidisciplinary perspectives put forward by the contributors. These multidisciplinary approaches are increasingly fundamental when it comes to understanding how different practitioners, organizations and countries are accounting for and mitigating the adverse effects of digital technologies in humanitarian crises and grappling with the unprecedented ways in which digital technologies are used as means and methods of warfare.

88 Victor Lukerson, "The Ethical Dilemma Facing Silicon Valley's Next Generation", *The Ringer*, 6 February 2019, available at: www.theringer.com/tech/2019/2/6/18212421/stanford-students-tech-backlash-silicon-valley-next-generation.

89 See, for example, Karen Hao, "An AI Saw a Cropped Photo of AOC. It Autocompleted Her Wearing a Bikini", *MIT Technology Review*, 29 January 2021, available at: www.technologyreview.com/2021/01/29/1017065/ai-image-generation-is-racist-sexist/; Ryan Steed and Aylin Caliskan, "Image Representations Learned with Unsupervised Pre-Training Contain Human-Like Biases", Carnegie Mellon University, 2021, available at: https://arxiv.org/pdf/2010.15052.pdf.

90 Eskild Petersen *et al.*, "Comparing SARS-CoV-2 with SARS-CoV and Influenza Pandemics", *The Lancet Infectious Diseases*, 3 July 2020, available at: www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30484-9/fulltext.

91 As a reference, see the new composition of the *Review*'s Editorial Board, available at: https://international-review.icrc.org/about/editorial-board.

92 *Ibid.*

The way forward

A key insight brought forth across many of the pieces in this issue of the *Review* is the need to assess and mitigate the risks of integrating new digital technologies into humanitarian work while undertaking digital transformation processes. As much as these tools bring certain benefits, they also pose irreversible risks, and there is a "dark side" to the use of digital technologies in humanitarian crises. There is also another aspect to this theme: as digital technologies evolve and are used in armed conflicts and other situations of violence, there is an ever-present need to ensure that IHL is respected. Yet, the question remains: where do we go from here as humanitarians when it comes to digital technologies and war?

The director of digital transformation and data at the ICRC, Balthasar Staehelin, perfectly reflects on the future of digital technologies and war by asking: "Is data the 'new oil' – or the new asbestos? Will we live in a world of the Internet or of a splinter-net?"[93] As Staehelin highlights, however, whatever the answer may be, in the coming years and decades, "the ICRC will do its utmost to adapt to the exponentially growing impact of digital transformation with and for the populations it seeks to serve in war zones around the world. Their continued trust in the ICRC will tell us whether we have succeeded in responsibly leveraging the enormous potential of evolving digital technologies for their good."

In line with this key point made by Staehelin, most of the diverse issues covered in this issue of the *Review* come down to one key requirement of humanitarian action: trust. All throughout this issue, trust indeed emerges as the backbone of digital transformation in the humanitarian system – yet there is no quick fix to create it. Humanitarian organizations craft their humanitarian access on the basis of the trust that they create with local communities and authorities on a daily basis. By the same logic, the way the bonds of trust are affected by digital technologies should be considered with particular attention and care by all stakeholders working towards the use of "technology for good".

As we look forward, embracing digital technologies should not only be about adopting new technologies, but about ensuring that such technologies reinforce the bonds of trust that we as humanitarians build with affected populations, offering them new options to ensure their needs are met. To this end, we hope that this issue of the *Review* will inspire the design of innovative digital transformation strategies centred around and in collaboration with the people they are meant to serve.

93 Quote submitted by Balthasar Staehlin to the authors of this editorial.