



presents a White Paper on

When Technology Meets Humanity: Shifting Policy Towards Protection in Conflict

How new and emerging technologies can be harnessed at the end of conflict

Prof. Laurie R. Blank, Emory University School of Law

Dr. Daphné Richemond-Barak, Lauder School of Government, Diplomacy and Strategy, Reichman University

November 2024

White Paper Synopsis

Channeling new and emerging technological capabilities can offer significant contributions toward facilitating the end of conflict and protecting and easing the effects of conflict on the civilian population. For several years, the End of War Project explored and highlighted the potential that new and emerging technologies have as protective, cooperative, and effective tools as conflicts end or *begin* to end, a potential often overlooked amid the primary focus on how technology can make fighting in war more effective.

This White Paper presents the insights gained from several academic and policy-oriented events and provides specific recommendations on how to channel new and emerging technologies for good at the end of war. Many of these recommendations are also relevant to the use of technology for humanitarian purposes during war.

The role of new technologies in targeting – including GPS-guided weapons, battle networks, collateral damage estimation methodology (CDEM), cyber, drones, and autonomous weapons – has been the focus of extensive analysis by security and legal scholars. This scholarly literature has pointed almost exclusively at the use and effects of such technologies for targeting, with only limited attention being paid to the use of technology for easing the effects of war on the civilian population. Although emerging technologies have significant potential to enhance humanitarian and security objectives

during and at the end of conflict – just as they already do effectively in disaster management and relief – such opportunities have received little to no attention.

To this end, the End of War Project has identified a need to shift the discourse on the role of technology in wartime and place greater focus on how technology can be used to promote humanitarian values, particularly at the end of war.

In this White Paper, we

- draw attention to a significant scholarly and policy gap related to the use of technology at the end of war;
- show that existing and emerging technologies have the potential to assist and protect vulnerable communities at the end of war;
- provide real-life illustrations of how technology has in fact been used to further humanitarian values and protect civilian communities in areas of conflict (for example by limiting human trafficking risks for refugees and internally displaced persons or safeguarding communication among humanitarian actors); and
- make recommendations to help spur a policy shift and the development and deployment of new technologies at the end of conflict.

The End of War Project – Background

Led by Professor Laurie Blank at Emory Law School and Dr. Daphné Richemond-Barak at the Lauder School of Government, Diplomacy and Strategy at Reichman University, the End of War Project is a multi-year project designed to explore a range of legal, policy, moral and strategic challenges arising at the end of conflict.

The end of war is both a temporal concept and a substantive concept. As a temporal matter, the end of war refers to the spectrum of time from the winding down of conflict, through the formal or informal conclusion of the fighting, to the early post-conflict phase. The end of war therefore includes both periods of conflict and periods of peace.

Substantively, the concept of the end of war includes a plethora of challenging policy, legal and strategic issues, such as identification of the actual end of a conflict as a legal and factual matter, the release and repatriation of detainees, accountability for international crimes, rebuilding of civilian infrastructure and capacity, humanitarian assistance for displaced and vulnerable populations, and much more.

In particular, the end of war introduces significant uncertainty about the law that applies to and regulates the actions of the parties to the conflict, protects individuals and communities, and determines the authorities and obligations of states and armed groups, among other actors. During armed conflict, the law of armed conflict applies to regulate the conduct of hostilities and the protection of persons — but once the armed conflict ends, the law of armed conflict ceases to apply, with limited exceptions. At the same time, international human rights law applies, protecting individuals from the arbitrary deprivation of their rights by the state, and in situations of occupation, the law of belligerent occupation applies until the end of the occupation. The host nation or territorial state’s law

also applies – and countless other specific legal rules or frameworks will apply to particular events or issues arising across and at the end of conflict.

Beyond the challenge of navigating this complex legal landscape, the end of war poses unique challenges driven by the uncertainty inherent in conflict endings — including the complex determination of exactly when a conflict ends and, if more than two parties are involved, whether it ended for all groups at the same time. Recent and current conflicts testify to this complexity: the conflict in Syria has defied easy characterization and the question of whether and when it has ended and for which groups remains unanswered; the conflict between Azerbaijan and Armenia flare up repeatedly over decades; the conflict between Ukraine and Russia has been lasting with varying levels of intensity since 2014; conflict in Colombia appears to be simmering again; and the conflict between the United States and al Qaeda and other terrorist groups has been termed a “forever war” partly because no effective tool for identifying an end to the conflict has yet been accepted.

The fact that some of the issues explored throughout the project are not exclusively limited to the end of war but also arise during conflict does not detract from the project’s contribution: the uncertain legal and strategic landscape during the temporal timeframe of the end of war – which combines periods of conflict and early post-conflict peacetime – makes each of these issues more complex and introduces unique questions and considerations. At the most basic level, multiple legal frameworks may apply — or appear to apply — to a host of protection and implementation issues during this end of conflict timeframe, requiring an examination and deeper understanding of how this shifting legal landscape drives policy choices and the protection of all persons caught up in the maelstrom of war.

Focus on Technology and Humanity

The role of new and emerging technologies at the end of conflict was the End of War Project’s thematic focus from 2021-2023.

The lack of any substantive discussion about the use of technology to enhance the protection of civilian populations caught up in conflicts and facilitate the end of war has been striking. Although the United Nations and the International Committee of the Red Cross¹ are already using new technological capabilities for several of these purposes, and NATO has held simulations on the use of artificial intelligence in disasters,² the conversation too often focuses on the downside of technology rather than its potential upsides. This gap is felt on the ground, in the scholarly literature, the shaping of policy priorities, and the allocation of resources.

¹ICRC Biometrics Policy (2019) (file:///C:/Users/DELL/Downloads/icrc_biometrics_policy_adopted_29_august_2019_.pdf).

² NATO, *Remarks by NATO Deputy Secretary General Rose Gottemoeller at the Xiangshan Forum in Beijing, China*. 25 October 2018). [NATO - News: Deputy Secretary General Rose Gottemoeller in Beijing: “We need to defend ourselves in the digital age, and in the age of artificial intelligence”, 24-Oct.-2018](#); and *NATO Demonstrates New Technology to Counter Terrorism in Crowded Venues*. May 25 2022. https://www.nato.int/cps/en/natohq/news_195801.htm.

One underlying purpose of the law of armed conflict is to regulate and limit the effects of conflict so as to enable the warring parties to disengage and return to peace. In essence, a long-term benefit of the law's detailed rules for the protection of civilians, civilian infrastructure, religious and cultural property, and the environment is to preserve conditions on the ground that make a more durable peace between the parties possible. New and emerging technologies offer untapped opportunities in this regard, particularly as a conflict winds down and as the complicated process of post-conflict peace restoration begins.

Notably, the challenges encountered at the end of conflict resemble those experienced in humanitarian crises of various types, including major floods and earthquakes that lead to massive destruction of infrastructure and uncontrolled displacements of populations. Highlighting the potential of technology in such contexts therefore presents some clear advantages, given the common use of technology in humanitarian action. Implementing such technologies at the end of war would not constitute a major departure from existing practices. It is feasible, but it requires a shift in how resources are allocated and priorities set.

This project engaged with multiple stakeholders (humanitarian organizations, military, and scholars) to expose how technology can be channeled to facilitate the end of war by reducing uncertainty and vulnerability and enhancing trust among the parties.

The Project's activities on this thematic focus included:

- *Can Technology Bring About the End of War?*, with Prof. Eric Jensen, Dr. Jacob Stoil and Dr. Larry Lewis (online December 2020), as part of the End of War Project's **Fall 2020 Global Dialogue**:
 - Co-sponsored by CNA, this event launched the thematic focus on the role for new and emerging technologies at the end of conflict. With an interdisciplinary exploration of historical context, legal and ethical considerations, and policy imperatives and objectives, the discussion highlighted the need for deeper exploration of a broad range of opportunities across the end of conflict spectrum.
 - Key insights from the event were published in *Technology, Humanity and the End of War*,³ which lay the foundation for what would become a long-term, dynamic, and ground-breaking exploration of how emerging technology (AI, blockchain, biometrics and others) can be used to advance humanitarian goals and facilitate the transition from war to peace.

- *When Technology Meets Humanity: Exploring How New and Emerging Tech Can Facilitate and Protect at the End of Conflict* — March 2022
 - In cooperation with the Lieber Institute of Law and Land Warfare at West Point, the End of War Project convened a multi-disciplinary conference

³ Laurie R. Blank, Eric Jensen, Daphné Richemond-Barak, and Larry Lewis, *Technology, Humanity, and the End of War*, ARTICLES OF WAR, May 26, 2021, <https://lieber.westpoint.edu/technology-humanity-end-war/>.

with experts from law, security studies, international relations, ethics, cyber, civil engineering, philosophy and history for a dynamic and innovative exploration of four core themes:

- Identifying and addressing the population’s needs
- Data collection and processing
- Sharing and safeguarding information
- Detainees and refugees
- The goal was to identify how technology can help resolve real-life dilemmas specific to the end of conflict, and how law may promote – or at least not hinder – such uses of emerging technologies, from bolstering efforts to end conflict to facilitating the winding down of conflict and enhancing protection and capacity-building in the immediate aftermath of conflict. This two-day gathering helped refine the types of technology concerned, the unique types of challenges encountered at the end of war, and the limits (legal, ethical, or otherwise) of emerging technologies. Participants discussed potential solutions to concrete on-the-ground challenges that would make use of specific technologies.
- *When Technology Meets Humanity: Democratic Resilience at the End of War* — June 2022
 - This second gathering of experts, at Reichman University in June 2022, broadened the scope of the discussion to a non-American audience. Co-sponsored by the American Red Cross and the Program on Democratic Resilience and Development at Reichman University (in partnership with the Konrad Adenauer Stiftung), this two-day international conference was built around well-defined scenarios and sought to reach policy recommendations based on the preliminary findings from the West Point roundtable. Participants from Europe, Israel and the United States addressed concrete questions in plenary discussions and small group brainstorming sessions. They wrestled with the most difficult issues arising at the end of war and highlighted the promise (and problems) they foresaw using technology to address such issues.
 - Our piece, [*Putting Technology to Work for Humanitarian Purposes in War*](#), published in the National Interest, distills insights from this second event.⁴
- A draft of this White Paper was released to a limited group of participants ahead of the World Summit on Counter-Terrorism in September 2022 for additional feedback and later discussed at a public event in the presence of several humanitarian organizations. Insights gained at this capstone event have been integrated into this White Paper.
- An interactive policy pitch for the development and deployment of AI to reduce harm to civilians and ease the effects of war was presented at REAIM 2023, a

⁴ Laurie Blank and Daphné Richemond-Barak, *Putting Technology to Work for Humanitarian Purposes in War*, NATIONAL INTEREST, July 9, 2022, <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/putting-technology-work-humanitarian>.

conference on responsible AI in security organized by the Ministry of Foreign Affairs of the Netherlands and South Korea in The Hague.

- Insights from an interactive discussion with the audience, using the BetterBeliefs technology, were summarized in *Responsible AI Symposium – Prioritizing Humanitarian AI as Part of “Responsible AI”*.⁵
- Insights from the project and the White Paper were presented at the Institute for Ethics in AI, Oxford University in February 2024 (*Humanitarian AI*).

This White Paper is thus the product of a unique multi-disciplinary and multi-stakeholder process bringing together lawyers, humanitarian actors, experts in various technologies, representatives of the private sector, military officials, philosophers, and security scholars. The recommendations presented below draw from hands-on feedback provided by these experts over the course of multiple encounters and focused discussions, and the comments and criticisms that emerged from small group discussions and collective participatory data collected via the BetterBeliefs platform.

With this White Paper, the End of War Project seeks to engage actors and organizations across the arenas of war, humanitarian action, and technology, to help channel the discourse about and use of new and emerging technologies towards the protection of persons and communities as conflicts wind down and peace is nurtured and restored. Lawyers, policymakers, advocates, developers, humanitarian actors, military officers, and academics – all are critical contributors to this conversation. Across these multiple and intersecting sectors and audiences, it is critical for individuals and organizations who believe in the promise of technology for protective and cooperative purposes in and at the end of war to engage and drive new research, programming and action.

Identifying Technology

In considering how technology can be used to meet overarching goals at the end of war, an essential predicate question is what key functions are needed in the end of war space — for civilian protection, for interactions between or among warring parties, for enhanced humanitarian response, and more. Mindful of the speed at which emerging technologies evolve and the need to be constantly attentive to any underlying ethical or legal concerns, several current and emerging technologies are of particular relevance in this context:

- *Machine learning tools to aid assessment and decision-making.* Machine learning tools can help process volumes of data from a variety of sources (public and non-public, government and civil society), fuse information, and help identify patterns that may not be obvious to humans. These tools are not necessarily suited for making decisions; rather, they can help provide additional context and insight to inform human decision-making.

⁵ Daphné Richemond-Barak and Larry Lewis, *Responsible AI Symposium – Prioritizing Humanitarian AI as Part of “Responsible AI”*, ARTICLES OF WAR, March 17, 2023, <https://lieber.westpoint.edu/prioritizing-humanitarian-ai-responsible-ai/>.

- *Machine learning tools to optimize functions.* Machine learning can also be used to solve specific complex problems, such as optimization of supply chain management, allowing more efficient and adaptive use of available resources. The same tools could be used to speed up the delivery of foodstuffs and medical supplies in war-torn areas.
- *Blockchain.* A blockchain is a distributed approach to securing transactions using computing power and exchanges between trusted participants, creating a secure, shared and immutable tool for recordkeeping between and among disparate entities. These exchanges are auditable, making this approach useful for evidentiary purposes. Within alliances but also between warring parties, blockchain minimizes misinformation, increases trust, and guarantees the validity and security of the information shared.
- *Autonomous systems and remotely piloted vehicles.* Pilotless vehicles can provide capabilities such as surveillance or logistics with greater persistence and without risk to human operators. Remotely piloted air, land, or sea vehicles can access areas where communication is limited, personnel for the platforms is unavailable or affected communities have become isolated (for example where roads have become unusable) as a result of the conflict. Drones can be used to deliver medical supplies to populations affected by conflict or even blood to wounded people, as already tested in Rwanda.⁶
- *Biometrics.* Biometrics can be a powerful tool for providing humanitarian aid, with appropriate attention to and safeguards regarding data security and human rights. For example, fingerprints, DNA, or retinal scans could be employed for registering displaced persons and finding more efficient ways to tailor and deliver assistance. Facial recognition software, in particular, may be used to identify victims, help families unite in the wake of the conflict, and enhance medical treatment by allowing medical teams to quickly access medical records.
- *Satellite imagery.* Satellite imagery can and has been used to collect information about the location of atrocities and the commission of war crimes.⁷ This technology holds unique promise in the field of accountability – allowing the verification of facts, even long after the conflict has ended.⁸ Satellite imagery may also effectively document troop movement and damage to cities.

⁶ *Technology in Rwanda: How Drones are Saving Lives*, 9 January 2022, <https://www.borgenmagazine.com/technology-in-rwanda>.

⁷ Malachy Browne, David Botti, and Haley Willis, *Satellite Images Show Bodies Lay in Bucha for Weeks, despite Russian Claims*. N.Y. TIMES, April 4, 2022.

⁸ Roya Pakzad, *Opportunities and Challenges of Emerging Technologies for the Refugee System*, Center for International Governance Innovation, 2019, https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20No.11_1.pdf (noting that "[b]y analyzing global positioning system data and satellite imagery, interviewing witnesses through Skype video-chatting and scrutinizing high-resolution images from local activists, the Human Rights Watch team concluded that the attack was most likely delivered by Bashar al-Assad's regime.")

This list is by no means exhaustive. However, it offers a set of tools to highlight and analyze how these advantageous and even unique capabilities could be leveraged to preserve public order, tend to affected populations, and stabilize the security environment across the spectrum of ending conflict, from preparing and then facilitating the end of conflict to supporting the restoration of peace.

Most importantly, the development and use of technology must be matched to the needs of the population, decision-makers and other actors involved at this stage of conflict. This match between on-the-ground needs and technology is the key to adaptability, accessibility and, ultimately, effectiveness.

Concerns

Channeling the potential of technology for good is a cautionary tale. Technology introduces risks and creates vulnerability: what happens when the technology does not work, or mistakes occur? Throughout the project discussions, experts highlighted the need to balance the potential of emerging technologies with a sober recognition of ethical and legal considerations that can arise. In any situation, technology comes with a level of risk that must be managed. No technology is foolproof, and no solution comes risk-free. It was agreed that the potential of technology ought to be channeled, and potential risks mitigated.

- *Privacy and Human Rights.* Many of the technological opportunities involve the collection, storage and use of massive amounts of data about individuals and communities that are vulnerable, displaced, and subjected to ill-treatment and violence. Although new and emerging technologies offer extensive opportunities to mitigate harm to such individuals and communities, as discussed below, they also risk infringement on individual rights. Biometrics and other tools for gathering, storing and analyzing personal identifying information present significant concerns regarding privacy. In the hands of hostile actors, personal information contained in biometrics can be extraordinarily dangerous; it is also vulnerable to hacking and other security breaches. Steps can and have been taken in the past to mitigate these concerns, such as the destruction of biometric data belonging to displaced persons or refugees to protect their information and safety.
- *Over-reliance and Over-generalization.* Technology can appear to be a quick solution to difficult challenges without a full understanding of those challenges and the important cultural, geopolitical, geographic and other contexts at play. Importantly, technologies developed for one situation, region or conflict are not necessarily well-suited for other situations, and their hasty implementation could create gaps or even distrust. In addition, an over-reliance on technological tools can lead to blind spots and a lack of appropriate verification mechanisms, opening the door to misinformation and disinformation.
- *Dependency.* At the same time that new and emerging technologies can create efficient and advanced solutions to large challenges, they can also leave individuals, organizations and communities dependent on such tools if they do not build in

protections and backups in case of failure, sabotage or other problems. Experts cautioned that such dependency can leave vulnerable groups with no assistance, so organizations and governments must be prepared for such shutdowns and have plans in place to enable critical humanitarian programs to continue when technologies face interference or destruction. The hack against the ICRC not only compromised the personal data of countless civilians, it also brought the organization to a halt.

Additional concerns mentioned by consulted experts include the risk that technology will not be distributed equally among countries and conflicts. Others fear that mistrust in technology and government will have a negative impact on how technology is perceived by the public and humanitarian organizations alike and emphasized the need to educate and train affected population in the use of technology.

Concerns will undoubtedly arise from the use of new and emerging technology during and towards the end of conflicts, even if the aim – upholding humanitarian and democratic values – is a laudable one. While these concerns must be acknowledged and addressed, this White Paper deliberately takes the uncharted route of focusing on opportunities and advocating a problem-solving approach. As noted above, this approach aligns with the view of many participating experts that concerns can be mitigated.

The threat of human trafficking that followed Russia’s invasion of Ukraine offers a case in point. Many women and children who sought refuge in Moldova found themselves vulnerable to individuals who offered to take them to safe places within the country. DigitalLink, the philanthropic arm of Monday.com, a technology company focused on creating operating platforms for companies, stepped in. They set up a system that required drivers to share personal information prior to picking up refugees. The women then registered a drop off address, which was later verified when they were dropped off by the driver. This system limited the risk of human trafficking and increased the safety of the refugees. Although it could have been exploited by certain actors and was not foolproof, it helped considerably with the use of rather basic technological tools.

Similarly, records of refugees collected by humanitarian organizations for their protection could end up in the wrong hands and biometric data used for facial recognition can lead to racial profiling and surveillance. The potential for misuse can and must be mitigated but it can never be fully eliminated. Mitigating steps that have been put in place include safeguards in data collection to make sure that only data that is absolutely indispensable is collected, built-in systems to report concerns and complaints, and the destruction of data to avoid privacy breaches.

In our view, a policy shift on the use of AI in conflict must come with the willingness to actively pursue solutions and anticipate and mitigate risks or concerns that arise. The process of seeking and implementing tech-supported solutions must bring together the variety of actors involved during and in the aftermath of conflicts – governments, militaries, humanitarian organizations, international actors, and more. Participation brings trust in the process, and in the technology. These actors need to be involved in the collection

of the data, and informed regarding how the data will be stored, used, and potentially even transferred.

Findings and Analysis

Identifying fruitful avenues for new and emerging technologies to contribute at the end of conflict rests on two main inquiries. First, understanding the range of challenges that civilians, warring parties, humanitarian organizations and other actors face in that complex and shifting space is essential to assess the needs and gaps in protection. The second piece is to explore the possible uses of technology to address those needs and gaps – in essence to “match” problems and opportunities.

The End of War Project’s interdisciplinary approach is a critical component for this process, bringing together humanitarian practitioners, international lawyers, military lawyers and commanders, and technology developers and experts to maximize cross-pollination of ideas, challenges, and recommendations.

This section presents five main categories in which the opportunities for new and emerging technologies to contribute at the end of conflict are significant. It then highlights some concerns to address in any further development or implementation going forward.

Key Opportunities

1. Facilitating the End of Conflict

The law of war’s core rules and protections are critically important for minimizing harm to civilians during armed conflict. But bringing a conflict to an end — which brings an end to exchanges of artillery, attacks on targets in populated areas, detention and internment, and many other features of armed conflict — is, of course, the obvious and comprehensive way to help protect civilians. Many contemporary conflicts, however, seem to perpetuate, running hot and cold or simmering for years and even decades.

New and emerging technologies can play an important role in minimizing uncertainty at the end of conflict, which can be a substantial obstacle to progress towards peace — uncertainty about whether the strategic picture allows for negotiation or other action to try to end the war and uncertainty about whether the adversary is abiding by negotiated ceasefires and other agreements. Autonomous systems, drones, and satellite imagery can gather credible information on damage in conflict areas and the movements of fighters and civilians, creating an accurate picture for decision-makers to consider, and machine learning tools can then analyze such data—potentially even in combination with data gathered from other sources.

More important, in many cases, ending a conflict means avoiding escalation. Warring parties often cause more violence as they seek to end a war or tensions rise as atrocities are discovered or commitments appear unfulfilled. Imagine technological tools that

could enable the parties to verify and trust information about the position of forces, the adherence to ceasefires, or the demobilization of forces, such as blockchain and other means of securing information flows. Mitigating uncertainty can help smooth the path to peace by removing common obstacles and sources of re-escalation.

For example, ceasefires can fail due to accidental or small unit violations, which are primarily the result of ill-informed tactical commanders or rash actions, or intentional violations, which are significantly more problematic. Mapping unit positions at the immediate moment of cease fire and using all-platform messaging of an agreed-upon mutual translation of the ceasefire terms can help make sure that all parties, even down to the tactical level, are aware of the ceasefire and its terms, and that small units do not continue to fight. Such tools can help build trust by ensuring that all actors know where their own forces and the adversary's forces are. Technology can also, and perhaps more intuitively, enable constant monitoring and recording of border incidents or other flare-ups – thereby avoiding escalation and enhancing stability.

Other opportunities for new and emerging technologies include facilitating a more orderly and resilient demobilization, disarmament and reintegration (DDR) process through tracking of disarmament and more targeted reintegration by region, sector and skill set. Organizations and government agencies can provide remote psychological first aid for former combatants and civilians. Algorithms can predict refugee paths based on patterns and weather, allowing relief organizations to be proactive rather than reactive, anticipate crossings and other mass movements, and better allocate resources accordingly. International organizations, governments and relief organizations can use technology to better map conflict areas to generate maps catering to different needs and vulnerabilities, such as disability, gender, safe areas, and more.

As conflict winds down and as the complicated process of post-conflict peace restoration begins, these are just some examples of how technological capabilities can facilitate the end of war and ease the transition from war to peace.

2. Sharing and Safeguarding Data and Information

New and emerging technologies can facilitate the sharing and safeguarding of information and thereby improve the ability of former adversaries to engage with each other in a more productive manner to help maintain a tenuous peace after hostilities cease.

Identifying the needs of vulnerable populations, managing the flow and security of information during negotiations, or tracking the return of displaced populations — throughout the end of conflict space, data and information is omnipresent and of critical importance. As the experts at both roundtables noted, different stakeholders have different needs for information, different levels of willingness to share information, and different relationships to the individuals or communities whose information they collect and use. For example, humanitarian organizations produce enormous amounts of information, but often lack the in-house capacity to analyze and process it. Militaries and governments naturally are reluctant to share information and international organizations have their own

imperatives and limitations with respect to the data they gather and use. Importantly, the law applicable to the data might change if and when such data is transferred to a foreign actor.

One consistent concern across the temporal scope of the end of conflict and the many actors involved or affected is trust — trust in the validity and secure use of information. Blockchain and other developing tools offer numerous opportunities for secure shared information and communications platforms. For example, blockchain can help track donations and ensure that aid earmarked for a certain purpose or recipient gets delivered accordingly.

As populations move away from conflict, monitoring their movement is essential – but also potentially a grave threat to their security. New technologies can help to predict, assess, and manage the flow of persons and contribute to a more efficient and supportive program for assisting displaced people and refugees. The rush of assistance offered to civilians fleeing Ukraine, mentioned above, helped to support refugees at a highly uncertain time. Such solutions could easily be expanded upon across similar situations.

Knowing the number, medical condition, linguistic needs — along with many other important features — of displaced communities is critical for the provision of supplies, housing, transportation, services, and other basic assistance. At the same time, however, that same information in the hands of a state or other actor can be extraordinarily dangerous. As an example, the United Nations High Commissioner for Refugees has collected massive amounts of biometric data on Rohingya refugees who fled Myanmar into Bangladesh.⁹ As UNHCR negotiates for their return to Myanmar, consider the risk of that biometric data being transferred or otherwise falling into the hands of the Myanmar authorities. Refugees and displaced persons generally have no choice but to share their biometric and other data to receive services and assistance, but that data then makes them vulnerable to exploitation, abuse and other harms if it lands in the wrong hands.

Other key issues include developing systems for interoperability in the information space, both among like organizations (humanitarian to humanitarian or state to state) and across sectors. Technology can help here with building a shared vocabulary and lexicon, translations, and building trust among actors working in the same space.

3. Enabling and Enhancing Humanitarian Action

Humanitarian organizations face extraordinary dangers operating in wartime and post-conflict environments. In many areas, they face the challenge of how to notify friendly forces of their location while protecting that location from discovery by hostile forces. Technology to enable encrypted notification and sharing of location and other critical

⁹ *Tagged, Tracked and In Danger: How the Rohingya Got Caught in the UN's Risky Biometric Database*, WIRED UK, March 12, 2018, <https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh>.

information will help to protect humanitarian workers and organizations and thus enhance their ability to help populations in need.¹⁰

Humanitarian experts also expressed the need to communicate on safe, user-friendly platforms that verify the identity of actors and of the information communicated. Blockchain, a decentralized database which stores a registry of assets and transactions across a peer-to-peer network, could answer such needs.¹¹

Data protection is another daunting task for humanitarian organizations. As the International Committee of the Red Cross recently noted, “humanitarian organizations are exposed to a growing wave of digital attacks and cyber espionage and have become highly prized targets.”¹² In 2022, data held by the ICRC was compromised by a cyber-attack of unprecedented proportions against a humanitarian organization.¹³ The data breach revealed the need to find solutions to protect the data of those who are most vulnerable, including those separated from their families due to conflict or disaster.

Relatedly, understanding how misinformation and disinformation can affect the perception of humanitarian organizations as neutral and impartial can help to forestall problems of distrust among assisted populations and warring parties – and further contribute to building trust.

4. Accountability and Redress

The international criminal justice field is already deeply engaged in the use of new technological tools to assist with the gathering, storage and processing of information about atrocities and other harms committed during armed conflict and other situations of violence. In Ukraine, for example, Bellingcat and other actors have set up networks for the sharing and receipt of data, photographs, and videos about atrocities committed by Russia, for future use by the International Criminal Court or other courts and tribunals. Satellite imagery and drones can be and are used to gather evidence, and new databases and repositories are being created in real time to store information in a manner that they can then be admissible in a court of law.

A range of additional challenges arise in this space that present opportunities for new and emerging technological capabilities to further enhance international action. For example,

¹⁰ Larry Lewis and Daphné Richemond-Barak, *Could Emerging Technologies Have Helped to Avoid the Tragic Killing of Humanitarian Workers in Gaza?*, Modern War Institute, April 25, 2024, <https://mwi.westpoint.edu/could-emerging-technologies-have-helped-to-avoid-the-tragic-killing-of-humanitarian-workers-in-gaza/>.

¹¹ *Data Trust Methodology: A Blockchain-Based Approach to Instrumenting Complex Systems*, August 5, 2020, <https://www.ll.mit.edu/r-d/publications/data-trust-methodology-blockchain-based-approach-instrumenting-complex-systems>.

¹² ICRC, *Symposium Report: Digital Risks in Armed Conflicts*, Geneva, October 2019, reprinted in ICRC Review, <https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/Digital-technologies-and-war-IRRC-No-913.pdf>.

¹³ *Sophisticated Cyber-Attack Targets Red Cross Red Crescent Data on 500,000 People*, January 19, 2022, <https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people>.

humanitarians are first on the ground after devastation and conflict, meaning that they are witnesses to the destruction caused and abuses committed and deeply engaged with the populations that have suffered such harms. Registering evidence or testifying before a criminal tribunal is not in the mandate of such organizations, but tools can be developed to prevent the loss of that valuable information without compromising the posture of relief workers. Some have suggested the development of a common open-source questionnaire that organizations can use with displaced and vulnerable populations to help with the collection of information. Similarly, a database that is centralized to input witness and victim statements — such as those in use by CaseMatrix or CaseMap — can prevent duplication of effort and include cross-referencing and other capabilities to maximize value for investigations and prosecutions.

Criminal accountability is only one aspect, however. Redress and reparation, which are critical steps in the post-conflict process, depend on information and reliable records to ensure that individuals can recover their assets or property. Unsecured means of collecting and storing such information can place these individuals in even more vulnerable positions, open to theft, scams and other criminal mischief. Equally problematic, most individuals fleeing from conflict and other danger do not have the time or the means to locate and bring with them documentation of their assets, banks accounts, property, etc. Technology that stores such information in an encrypted and secure manner can contribute significantly to redress and restitution efforts. As noted above, it can also be used to ensure that displaced persons, asylum seekers, refugees and others are actually receiving the redress and assistance to which they are entitled.

5. Rebuilding and Reducing Vulnerability

During war, any and all tools to reduce vulnerability are essential. Civilians are vulnerable to attack and starvation, internment, disease, adverse weather, and many other hardships. Combatants captured by the adversary are also vulnerable—to mistreatment, loss of rights and privileges, disappearance, and other harms.

Any tools that can minimize such vulnerabilities must be harnessed, and we have identified three main areas where technology can be most helpful in mitigating the impact of conflict on vulnerable populations and the hardships that arise as conflicts come to an end:

- *Damage to infrastructure, humanitarian response, and rebuilding*

Satellite imagery and enhanced data processing capabilities can enable a more accurate assessment of the damage caused to civilian infrastructure, in real time, and thereby improve the quality of the response. Integrating data from varied sources can provide a more refined picture of civilian needs and state capacity, and identify roads that have been damaged and other civilian infrastructure that needs rebuilding.

Sophisticated platforms can help identify the basic needs of the population (such as employment, schools, and housing) and provide solutions by enhancing coordination and

community support. Aggregating data and making it accessible via a user-friendly dashboard has proved very useful in this regard.

Drone imaging technology equipped with remote sensors has been used in Uganda, for example, to produce “very high-resolution aerial photomosaic” which, combined with hazard, risk and vulnerability information and historical data on rainfall, has helped communities make better decisions as to which crops to grow and where.¹⁴ One can easily imagine how such solutions could help with land management and the resettlement of populations in the wake of conflict.

- *Family reunification and identifying the dead*

The ICRC’s *Trace the Face* program, an online tracing service with photos of people looking for their relatives, helps displaced people locate family members via a database of thousands of pictures, freely accessible online. The ICRC notes that “the application of artificial intelligence for facial recognition to automate searching and matching is revealing further potential of new technology to accelerate one of the ICRC’s core activities.”¹⁵

Facial recognition can assist with family reunification and the identification of the dead. Access to large datasets containing billions of photos that have helped Ukraine identify the dead. At the same time, the technology could be misused or abused – and has raised some concerns.¹⁶

- *Displaced persons and refugees*

Technology can be used to better predict and prepare for movements of population. An analysis of weather patterns, historical data, and information gathered from popular social media platforms can help identify the path that displaced persons will take as the conflict is coming to an end.

Biometrics are regularly collected by humanitarian organizations managing the records of refugees entering refugee camps and entitled to humanitarian aid. Of the more than 22.5 million refugees believed to be spread across the world, almost 20 per cent are registered on the Biometric Identity Management System of the UNCHR.¹⁷ Similar solutions could be implemented to assist populations who have been displaced and wish to return home and be reunited with loved ones at the end of war.

¹⁴ *Mapping for Resilience – Using New Technology to Map Oruchinga Refugee Settlement – Uganda*, ReliefWeb, May 5, 2016. <https://reliefweb.int/report/uganda/mapping-resilience-using-new-technology-map-oruchinga-refugee-settlement>.

¹⁵ *Rewards and Risks in Humanitarian AI: An Example*, September 6, 2019, <https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence/> and <https://www.icrc.org/en/document/trace-face-reuniting-families>.

¹⁶ *Ukraine Has Started Using Clearview AI’s Facial Recognition During War*, U.S. NEWS, March 13, 2022, <https://www.usnews.com/news/world/articles/2022-03-13/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war>.

¹⁷ *Biometric Identity Management System: Enhancing Registration and Data Management*, <https://www.unhcr.org/uk/protection/basic/550c304c9/biometric-identity-management-system.html>.

More specifically, blockchain technology has been used to administer humanitarian aid with greater transparency: a blockchain platform called BanQu has been designed to help Somali refugees in Kenya establish a permanent and verifiable digital identity using selfie photos, physical characteristics, biometrics and information about family members. This can be significant for victims of conflict who have lost all official records.

Finally, a Swiss team of researchers gathered data from refugee resettlement agencies in the United States and Switzerland. Based on refugees' background and skill sets, they were able to match refugees to a host city in which the individual has a higher chance of finding employment.¹⁸ Such programs can significantly improve resettlement efforts at the end of war.

Recommendations and Next Steps

- **Prioritize and focus.** Move past the focus on lethality and bring attention to tech as a force for humanitarian contributions and positive steps at the end of conflict. These capabilities are rarely prioritized in the same way as the tools of war. Governments and others should therefore make a deliberate choice to resource such capabilities.
- **Engage.** Engage with stakeholders to explore opportunities and obstacles.
- **Bring all stakeholders around the table.** Build trust among and between actors; focus on dialogue, trust, and interoperability.
- **Continue to identify needs on the ground.** Identify the needs of the population and those of the various organizations and actors involved.
- **Invest.** Invest and create opportunities for the development and deployment of technological solutions focused on key opportunities: facilitating the end of conflict, sharing and safeguarding data and information, enabling and enhancing humanitarian action, accountability and redress, rebuilding and reducing vulnerability.
- **Mitigating vulnerabilities.** As we work to enhance the positive impact of technology on the ground in conflict situations, it is important to keep in mind that the implementation of technological solutions at the end of war should not exacerbate existing vulnerabilities or create added dependencies.

¹⁸ Roya Pakzad, "Opportunities and Challenges of Emerging Challenges for the Refugee System," World Refugee Council Research Paper No.11, May 2019. https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20No.11_1.pdf (citing Kirk Bansak, Jeremy Ferwerda, Jens Hainmueller, Andrea Dillon, Dominik Hangartner, Duncan Lawrence and Jeremy Weinstein, *Improving Refugee Integration Through Data-driven Algorithmic Assignment*, SCIENCE 359 (6373): 325–29 (2018)).

- **Limit dependency; increase inter-operability.** Systems should be user-friendly and used with a view to guiding and teaching rather than creating dependency. Accessibility and interoperability among key actors are important requirements.
- **Avenues for further investigation and research.** Going forward, attention should be paid to investigating the differences between disaster and conflict from the point of view of applicable law, needs, and vulnerabilities. Assistance in conflict raises ethical and political issues that disasters do not. Tech companies will be wary of getting involved – even on a *pro bono* basis – in an ongoing conflict. Such involvement might be perceived as inappropriate; the company could be accused of “taking sides” or even be labelled a participant in the conflict; or such involvement could in turn affect incoming contracts and revenues. No such political considerations taint actions taken in the aftermath of a natural disaster. Disasters and wars also differ in how they impact vulnerable populations. Whereas victims of disasters will welcome technology that identifies their needs and location and accelerates the arrival of relief, war refugees may instead seek to avoid detection as they attempt to stay out of the hands of the adversary and reach a safe place. In addition, the use of a given technology (say, drones) for both lethal purposes and protective purposes in war could be perceived negatively by the population. Their use for protective purposes, for example to deliver supplies, food or medical aid, could trigger unwanted suspicion and fears. In contrast, the arrival of drones in situations of disaster will merely signal the delivery of aid and be welcomed by a population in need. The differences between the use of new and emerging technologies in disasters, on one hand, and in war, on the other hand, questions should be explored further to enable an efficient, protective, and safe use of technology at the end of war.

We hope that this White Paper will pave the way for more work on these important issues and spearhead a much-needed policy shift.

Conclusion

Modern technology can provide a real boost to family reunification through facial recognition software and other biometric tools, enhance identification of areas that require humanitarian relief and reconstruction assistance using satellite imagery, and help ensure that various fighting factions are aware, in real-time, of when and where ceasefires go into effect.

These possibilities account only for a fraction of how technology can assist at the end of conflicts – a timeframe that carries significant resemblance with the aftermath of disasters. If technology is used successfully to alleviate the suffering of victims and forge the path to recovery in the wake of earthquakes and floods, could it be used for similar purposes as conflicts come to an end?

Breaking the stigma that views technology in war as solely about attacks and lethality can enable international organizations, humanitarians, militaries, tech companies, and scholars to work together to shape this new and promising humanitarian role.

The multi-stakeholder process leading to the publication of this White Paper has demonstrated the need and willingness of militaries, experts, and humanitarian actors to come together and envisage how various technological solutions from blockchain to satellite imagery could provide solutions to challenges arising on the ground. These challenges include safe communication and trust-building among warring parties, record-keeping of atrocities, the implementation of cease fires by various factions, and more.

This White Paper purposefully places the emphasis on the opportunities rather than the challenges associated with the use of technology at the end of war. It does not seek to underestimate or downplay such challenges. On the contrary, efforts must be made to examine challenges and mitigate them. Potential downsides, legal and privacy hurdles, and risks of increased vulnerability should not impede the allocation of resources to the development and deployment of technologies that may alleviate uncertainty and vulnerability at the end of war. Resources, once allocated, should be directed towards an exploration of opportunities, alongside a genuine attempt at mitigating associated risks.

It is hoped that this White Paper, addressed to states, regional and international organizations, militaries, technology developers, and security experts, will serve as a catalyst toward a policy shift and a greater, more efficient, and safe use of technological solutions “for good” at the end of war.

Acknowledgements

Sponsors

The End of War Project would like to extend special thanks to CNA, the Lieber Institute for Law and Land Warfare at West Point, the Program on Democratic Resilience and Development at the Lauder School of Government, Diplomacy and Strategy (in partnership with the Konrad Adenauer Stiftung), and the American Red Cross for their generous support and contribution along the way.

Participants¹⁹

LTC Ronald Alcala, Lieber Institute for Law and Land Warfare, West Point
Audrey Alexander, Combating Terrorism Center, West Point
Dr. Ana Beduschi, University of Exeter Law School
Yau Ben-Or, Rural Senses

¹⁹ Please note that the inclusion of participants listed does not constitute endorsement by participants or their affiliated institutions or signify approval with all findings and recommendations contained in this White Paper. We do, however, wish to acknowledge their involvement in this process, and thank each of them for their valuable contribution.

LTC Andy Bellocchio, Department of Civil & Mechanical Engineering, US Military Academy
LTC Raymond Blaine, Cyber Research Center, US Military Academy
Dr. Russell Buchan, University of Reading
LTC Keith Carter, US Military Academy
MAJ Mehmet Coban, Department of Law, US Military Academy
Frank Coppersmith, Smarter Reality, CEO
Prof. Tom Dannenbaum, The Fletcher School
Prof. Chiara de Franco, Center for War Studies, University of Southern Denmark
Dr. Kate Devitt, BetterBeliefs
LTC Brian Drohan, Department of History, US Military Academy
Emanuela Chiara Gillard, Oxford Institute for Ethics, Law and Armed Conflict
Naama Gorodischer, ISRAAID
Camilla Guldahl Cooper, Norwegian Defence University College
Yael Vias Gvirsman, Harry Radzyner Law School, Reichman University (and EU Horizon 2020 NIGHTINGALE Project on Integrating Advanced Technology in Emergency Response in Complex and Mass Emergencies)
Christian Jorgensen, American Red Cross
Thomas Harper, American Red Cross
Prof. Eric Talbot Jensen, Brigham Young University Law School
Itamar Laist, Magen David Adom
Rob Lawless, Lieber Institute of Law and Land Warfare, West Point
Dr. Larry Lewis, CNA
MAJ Joe Littell, Army Cyber Institute, US Military Academy
Prof. Noam Lubell, University of Essex
Dr. Carmela Lutmar, Haifa University
Dr. Amichai Magen, Lauder School of Government, Diplomacy and Strategy, Reichman University
CPT Teddy McDonald, Department of Social Sciences, US Military Academy
Brigadier General David Mendelson, Assistant Judge Advocate for Military Law and Operations, U.S. Army
Tanya Murkes, SID Israel
Prof. Histoshi Nasu, Department of Law, US Military Academy
Lt. Col. Amy Nieman, National Security Law Division, Office of the Judge Advocate General, U.S. Army
Stephane Ojeda, ICRC in Israel & Occupied Territories
Dr. Magdalena Pacholska, Marie Skłodowska-Curie Postdoctoral Fellow, T.M.C. Asser Institute
David Polatty, Naval War College
Chen Raviv, Digital Lift
Nathaniel Raymond, Yale School of Public Health
Dr. Ido Rosenzweig, Minerva Center for the Rule of Law under Extreme Conditions, University of Haifa
Dr. Richard Schoonhoven, Department of Philosophy, US Military Academy
Dr. Yahli Shereshevsky, University of Haifa Law School
CPT Maggie Smith, Army Cyber Institute, US Military Academy

Sam Stevens, DT Institute

Dr. Jacob Stoil, Chair of Applied History, Modern War Institute at West Point

Dr. Diana Thomas, US Military Academy

Dr. Elad Uzan, University of Oxford

LTC Mark Visger, Department of Law, US Military Academy

Col. Winston Williams, US Military Academy

Nathalie Weizmann, United Nations Office for the Coordination of Humanitarian Affairs