frontiers | Frontiers in Human Dynamics

TYPE Mini Review
PUBLISHED 22 January 2025
DOI 10.3389/fhumd.2024.1465594

OPEN ACCESS

EDITED BY
James C. Simeon,
York University, Canada

REVIEWED BY
Roger Mac Ginty,
Durham University, United Kingdom

*CORRESPONDENCE
Ann Fitz-Gerald
afitz-gerald@balsillieschool.ca

RECEIVED 16 July 2024
ACCEPTED 18 December 2024
PUBLISHED 22 January 2025

CITATION
Fitz-Gerald A and Hennebry J (2025) Protecting civilians in a data-driven and digitalized battlespace: toward a baseline humanitarian technology infrastructure. *Front. Hum. Dyn.* 6:1465594. doi: 10.3389/fhumd.2024.1465594

Protecting civilians in a data-driven and digitalized battlespace: toward a baseline humanitarian technology infrastructure

Ann Fitz-Gerald[1]* and Jenna Hennebry[2]

[1]Political Science and the Balsillie School of International Affairs, Wilfrid Laurier University, Waterloo, ON, Canada, [2]Communication Studies and the Balsillie School of International Affairs, Wilfrid Laurier University, Waterloo, ON, Canada

This article examines the realities of modern day warfare, including a rising trend in hybrid threats and irregular warfare which employ emerging technologies supported by digital and data-driven processes. The way in which these technologies become applied generates a widened battlefield and leads to a greater number of civilians being caught up in conflict. Humanitarian groups mandated to protect civilians have adapted their approaches to the use of new emerging technologies. However, the lack of international consensus on the use of data, the public and private nature of the actors involved in conflict, the transnational aspects of the widened battlefield, and the heightened security risks in the conflict space pose enormous challenges for the protection of civilians agenda. Based on the dual-usage aspect of emerging technologies, the challenges associated with regulation and the need for those affected by conflict to demonstrate resilience toward, and knowledge of, digital media literacy, this paper proposes the development of guidance for a "minimum basic technology infrastructure" which is supported by technology, regulation, and public awareness and education

KEYWORDS

humanitarian assistance, emerging technologies, conflict, protection of civilians, basic technology infrastructure, humanitarian agencies, irregular warfare, digital and data-drive technologies

Introduction

This article examines conflict trends and the way in which contemporary wars are being fought in a data-driven and digitalized world. It notes an increase in irregular warfare, increased numbers of nonstate actors, and the increased use of technology-enabled weapons on all land, sea, air, space and cyber battlefields. The article examines some of the ways in which both security and humanitarian actors have adopted and use technology innovations, and argues that, in parallel with these developments and conflict trends, civilians have become more caught up in conflict than ever before. In acknowledging the challenge this leaves humanitarian actors in protecting civilians, we emphasize the need for guidance concerning a baseline technology infrastructure, with appropriate governance and accountability measures, to better support civilian protection in conflict-affected regions.

Trends and the future of conflict

Conflict trends continue to record the increasing toll that conflict has on civilian lives. This is explained by the locations in which conflict continues to take place, the nature of the conflict dynamics based on the objectives of conflict factions, the weapons used in conflict, and the positions occupied by civilian groups.

Scholarship which examines both conventional and unconventional - also referred to as "irregular" - forms of warfare (Smith, 2008; Kilcullen, 2012; Cordesman, 2016; Marks and Ucko, 2023) indicates that, while conflicts which have played out over the past 10 years include both conventional and irregular warfare, irregular warfare is on the rise. "Irregular warfare" is characterized as both warfare and armed conflict, inclusive of insurgency, counterinsurgency, terrorism and counterterrorism, and involves the credibility and/or legitimacy of the relevant political authority with the goal of undermining or supporting that authority (Larson, 2008, p. 7). Conventional warfare is more broadly understood as state-on-state conflict between organized, uniformed, professional military forces using massed firepower in open space away from civilians (Fabian, 2021).

Forms of irregular warfare, which have been observed in different parts of the Middle East, sub-Saharan Africa and Latin America, pose significant implications for civilians caught in this battlespace. Insurgency groups with both political and military objectives rely on the civilian population around them to assist in fighting the opponent. This reflects the Maoist model of insurgency which is based on a tight hierarchical control system, popular cohesion, and unconventional warfare activities to enable a resistance movement to disrupt or overthrow a government or occupying power (Kilcullen, 2016, p. 249). The model includes an 'auxiliary' component which interfaces with the local population to rally support for the cause, and to gather resources for the insurgent forces. In addition, an 'underground' component becomes responsible for more clandestine activities including intelligence and counterintelligence networks, special material fabrication, fund-raising, munitions, subversive radio, media networks, webpages, logistic networks, sabotage, and clandestine medical facilities (Joint Publication, 2016, p. 7).

What is different about today's irregular conflicts, such as insurgencies, is the way in which data-driven and digitalized processes have now widened the battlespace and globalized insurgency warfare across the virtual domain. These tactics have become further supported by transformative technology enablers such as Artificial Intelligence (AI), algorithms, and datasets which feed into machine-learning processes. At the same time, more conventional means of warfare have become empowered by these sophisticated technologies embedded in both conventional and autonomous forms of weaponry. The pace of production and use of these new technologies in all types of warfare has greatly outstripped the pace of well-developed governance and regulatory measures over their use and applications.

The role of technology in contemporary warfare

In addition to enabling weapons enhancements, the use of digital and data-driven technologies, such as AI, has also empowered information gathering to support what, in military parlance, is referred to as the "kill chain" (find-fix-track-target). These systems are used to operate precision-guided weapons and surveillance capabilities, which are now able to travel on unmanned aerial vehicles, all controlled from afar and supported by satellite data and built-in sensors that can interpret light, heat, sound and radio waves (Anonymous, 2024, p. 12). Targets become identified faster and more accurately, and drones – which have become a central feature of the 2022 war in Ukraine - become used for both persistent sensing and penetration into enemy space (Judson, 2023). Similarly, forms of psychological and informational warfare (Cohen et al., 2020, p. 52) have become more prominent and globalized by way of the internet, social media and the ability for any individual in the world to be both a producer and consumer of information.

Technologies such as the Government of Israel's "Project Lavender," an AI recommendation system designed to use algorithms to identify Hamas operatives as targets, have been used to track troops and battlefield movements (Schwarz, 2024). Another Israeli government-developed system named "Where's Daddy" has been used to track targets geographically (*Ibid*). In both cases, data is gathered through ongoing surveillance and targets become algorithmically determined. The US "Project Maven" has evolved from being a sensor program to an AI-enabled target recommendation system built for speed (*Ibid*). In all cases, targets are based on data from computer sensors and other sources to statistically and algorithmically assess what constitutes a potential target.

Data supporting advanced weaponry is also drawn from satellites such as SpaceX's Starlink satellites and those operated by the Finnish company ICEYE, which provide detailed radar images of Russian military positions (Anonymous, 2023). This means that even lower ranking members of conflict factions and civilians alike have access to connectivity and intelligence which, in the past, would have been restricted to higher ranking officers (*Ibid*). Civilian volunteers aiding the war effort can also participate in data collection exercises and drop location 'pins' onto apps such as the Ukrainian government's "eVorog" app (*Ibid*) – logging where and when evidence of artillery and troop movements are observed. Intelligence is also collected through the interception of cellular telephone discussions.

Biometric forms of data collection have been described as being central to counter-terrorism operations (Jacobsen, 2022). This data is highly sensitive and normally involves detection of a human iris and fingerprints. Armed forces use biometric data to inform wider security infrastructure, such as entry scanning machines which are used for entering military and diplomatic compounds. In Afghanistan, fingerprint data was taken from explosive devices to help identify individuals who had been involved in terrorist related attacks (*Ibid*).

While more dispersed networks of terrorist-related irregular fighters depend on information communication technologies (ICT), with primary emphasis on smartphones and cellular data to connect members and like-minded affiliate groups, the age of the internet has enabled many insurgency activities to work across the cyber domains. Zeitzoff (2017) discusses the use of social media to mobilize supporters, shape narratives, recruit, radicalize, and raise funding. Informational warfare aided by social media seeks to discredit perceived adversaries and bolster and recruit perceived potential supporters. The case studies of both Boko Haram in Nigeria and Al Shabab in Somalia have been profiled to demonstrate ways in which insurgents have exploited globalization to perpetrate terror (Adeyeye et al., 2022). Others have argued that the internet has been a boon for

insurgency groups based on it being rife with myths, and the rapidity at which ideas and information flow make it is impossible to gage the authority of any given source (Metz, 2012). The Putin government's disinformation campaign targeting the wife of French President Emmanuel Macron, which followed Macron's April 2024 statement concerning the possibility of deploying troops to Ukraine (Kostina and Pohorilov, 2024), serves as an example of targeted disinformation attacks by underground intelligence cells. The globalization of digital underground forces therefore fuels the internationalization of more localized and regional conflicts.

Civilians caught up in conflict

With conventional warfare now being fought using data, algorithms, sensors and the internet, with irregular warfare on the rise, and with most insurgency conflicts lasting an average of 12 years (Rabasa et al., 2011, p. xvi), the implications for civilians caught in such conflicts has further intensified. These trends combine with an increased use of technology by state actors, an increase in access to battlefield information by nonstate actors, and the rise of irregular warfare to widen and globalize the battlespace and involve civilian groups who, either knowingly or unknowingly, can become an instrumental part of a conflict faction's strategy. Warfare conducted in this digital and data-driven space also means that its onset of conflict no longer depends on who fires the first bullet or advances to the front line, but on ongoing activities taking place even during what appears to be peace time.

The reliance on data-driven and digitalized technologies has also placed a new focus on fighting in urban centers (Kilcullen, 2012). Based on the role played by capital cities in hosting critical technology infrastructure such as data farms, telecommunications and electricity compounds - and basic services such as medical centers - these become obvious targets in the fight for information supremacy. This intersects with increased migration of civilians affected by conflict to urban centers based on access to a wider aid ecosystem, friends and relatives, and transportation links. The 2023 fight for Khartoum between the Sudanese Armed Forces and the Rapid Support Forces (RSF) saw the RSF seize two data centers of the Sudani network (main government service provider) (CIPESA, 2023). By late 2023, approximately 70% of Sudan's hospitals and health centers were no longer functioning with only minimal services being offered by those that still were (CARE International, 2024). Similarly, reports accessed in June 2024 cited 1,442 attacks on health care centers across Ukraine.[1] Russia's April 2024 aerial attacks on Ukraine's energy facilities led to black-outs across different parts of the country and, by targeting the country's electricity grids and hydro-electric compounds (Hunder and Balmforth, 2024), increased the risk of an ecologically-driven humanitarian disaster and limiting civilian access to clean water, electricity for cooking, reliable information and heating, particularly during winter months. The targeting of basic and critical civilian infrastructure is a key tactic of insurgency warfare as it seeks to weaken legitimate authorities in the eyes of the wider population.

With approximately 86% of all Ukrainian targets reportedly being derived from drones (Anonymous, 2023), civilians also pay a high price for their dominant use in warfare. Weaponized drones operating in urban centers can cause significant collateral damage on civilians, especially drones which carry munitions like cluster bombs. In addition to the margin for error involved in machine-driven weapons system, both the unintended consequences of obscurants impacting satellite imagery which informs their targeting (Lichtman and Nair, 2015) and challenges associated with attribution (Lyons, 2012) raise numerous ethical challenges concerning the responsible use of these weapons systems. Scholars have underscored the need for rapid progress to be made on a new regulatory framework that places constraints on the development of any weapons that further diminish human agency over the use of force (Marijan, 2023).

While the collection of biometric data has been used by humanitarian actors to inform the distribution of food aid, admittance into refugee camps, and as proof of identification at border crossings, this has also presented risks for civilians caught in a fluid battleground with uncertain outcomes. This was the case in Afghanistan when, following the departure of NATO forces and the return of the Taliban-led government, the biometric data left by the interventionist forces was subsequently used to threaten and commit reprisals against those who had worked in support of the previous government and for NATO forces (Human Rights Watch, 2022). In the absence of data privacy laws in countries such as Somalia, the collection of biometric data by humanitarian groups such as the World Food Program (WFP) and the UN's Refugee Agency also posed risks for these involuntary data flows to fall into the hands of armed actors, such as Al Shabaab. The use of biometrics also brings security risks for refugee safety. As a result of not wanting to be identified at a number of informal checkpoints close to their route to Lebanon, many Syrian refugees actively avoided use of the official border crossing for fear that their details would be logged and accessible to those manning the informal checkpoints (Jacobsen, 2022).

Whereas civilians often rely on social media and messaging platforms to receive and send information, disinformation strategies have become a significant part of today's influence operations used by both state and nonstate actors. Social media, supported by enhanced AI-driven projection capabilities, is used as a vehicle to promote disinformation and propaganda. These strategies, which use intimidation tactics, can quickly silence civil society voices, affect social coherence, create information gaps and polarize communities (ReliefWeb, 2023). Amid complex and fluid environments, these influence operations can lead to communities losing faith in government institutions (UNSG, 2021), and even in the international agencies seeking to provide them with assistance. Disinformation operations can easily magnify and travel across the virtual space and through different global communities who support different conflict factions and who seek to influence the perspectives of the wider international community on a conflicts' dynamics. Social media platforms still lack the safeguards to prevent the distribution of false, manipulative and harmful content.

The use of technology in protecting civilians

The changing nature of conflict, a surge in technology-enabled weaponry and the use of new communication technology including

1 attacksonhealthukraine.org

social media, has created new challenges for humanitarian actors in negotiating access to affected populations and security for their own personnel (Wise et al., 2021). In parallel to these challenges however, these technologies have also created new opportunities for innovative responses.

Increasingly, humanitarian organizations, such as the International Committee of the Red Cross (ICRC) and Médecins Sans Frontières (MSF), rely on ICT and emerging technology to support their efforts in reaching and providing protection (e.g., relocation away from violence, access to asylum systems, temporary housing, etc.) and access to life-saving services and supplies to civilians during conflict (ICRC, 2022) as well as in response to climate crises. For example, remote sensing data and satellite imagery that has been used to assess risks of flooding and hurricanes, and to respond to climate and/or disaster-induced forced displacement, has also been used to assess conflict-related damage to houses and buildings. Notwithstanding the technical, analytical and political challenges surrounding its usage, satellite data has been used to map growth and change in refugee settlements (Quintana, 2023), track large movements of people (Lavers, 2021), shelling incidents, building damage and evidence for war crimes investigations (Lyons, 2012; Poole et al., 2023). Satellite communications systems have also been used when communications services are no longer working. The use of Starlink to provide connections to civilians in both Ukraine and Sudan serve as examples (CBC News, 2023; Joshi, 2023). GPS technology has also assisted the navigation of humanitarian shipments to ensure that aid is reached by intended recipients (Kaiser et al., 2003), as well as the tracking of forced displacement and refugee flows (Awan, 2020). The Ukraine government developed an app called "Diia" to provide the population with timely and updated information and the ability for citizens to use the app to update their own information and to access government services (Filipchuk, 2021).

While space-based technology systems have been employed by the military for many years, the "dual use" nature of these functions has driven forward a dependency on space systems for essential civilian services such as food production and supply, water, waste management (Zhou, 2023). In recognition of this 'dual use' of data, and the importance of protecting humanitarian workers accessing increasingly complex conflict-affected regions, some scholars have proposed establishing an interface for humanitarian organization to military AI intelligence, surveillance and reconnaissance systems (Trusilo and Danks, 2023). That humanitarian groups such as the World Food Program are now supported by organizations like Palentir, which is widely known for the role its software plays in US counterinsurgency and counterterrorism, suggests that these partnerships are already developing. It also underscores that, while AI can help analyze and interpret vast, complex data sets to improve projections and decision-making around protection, this still requires capacities, technologies and resources to utilize data effectively.

With the number of functioning mobile telephones used in the world today now only just falling short of the total global population, the in-built GPS within smartphones brings significant potential to use this data for the tracking of civilians caught in conflict, economic transactions and even the roots of infectious diseases. For example, Hübl et al. (2017) analyzed human movement and migratory patterns and routes of irregular migrants from Northern Africa and the Middle East with geo-tagged tweets. Mobile applications, chatbots and social media can create immediate feedback loops with affected communities; while digital cash can provide rapid and flexible assistance (OCHA, 2023a).

The distribution of mobile telephones, and public-private partnerships with telecommunications providers, have supported humanitarian innovation by providing feedback mechanisms, call centers, chat boxes and social media for civilian communities. These projects rely on partnerships between mobile operators and humanitarian partners and seek to support preparedness, prevention and recovery. The SOLIS Bot, a mobile-enabled WhatsApp chat box designed for Syrian refugees in Lebanon, enabled communication between the refugees and humanitarian organizations (Acland and Willitts-King, 2023).

Private sector and civil society organizations are also important in developing technologies for human protection. For example, the Migrant Offshore Aid Station (MOAS) was the first private-funded (through fundraising) organization to start Search and Rescue operations in the Mediterranean Sea using drone technology (MOAS, n.d.). Additionally, the existence of projects like refugee.info is important to provide accessible information for asylum seekers. The platform provides information (in multiple languages) for newcomers, rights, and family reunification in Bulgaria, Czechia, Greece, Hungary, Italy and Slovakia (Kaplan, 2018).

From assisting affected civilian populations to access services, to family tracing and reunification, efforts at the demobilization of child soldiers and facilitating refugee registration - new technologies offer powerful promise for humanitarian protection. However, the patchwork of access to, and application of, these technologies creates a very uneven playing field that may further inequities, and gaps in data, as well as human and technological capacities which continue to limit their widespread and efficient use. Incomplete data sets can lead to digital discrimination, while inadequate data responsibility can cause harm and generate mistrust (FRA, 2019). Inequities in connectivity, access to technology and digital literacy can exacerbate vulnerabilities and intensify gender and other biases (UN Women, 2024). Furthermore, populations facing emergency and conflict-affected situations are often absent from digital cooperation discussions and face additional challenges in achieving connectivity (UNHCR, 2016). Humanitarian actors will need to navigate a landscape with enormous volumes of data, including personal and other sensitive data, and increasing levels of mistrust, misinformation and disinformation (OCHA, 2023b).

Discussion

Extensive data connectivity and increased numbers of nonstate actors in conflict have led to a widened conflict battlefield. Within this widened battlefield, supported by digitalized and data-driven processes, the absence of data privacy laws and governance frameworks controlling a wider use of autonomous, data-controlled, and disinformation weaponry has increased and intensified ways in which civilians become 'caught in conflict".

Humanitarian groups have adapted their operations in the face of the new digital and data-driven terrain, particularly in terms of "mapping and tracking," and in analyzing evidence of human rights abuses and war crimes. Other uses of transformative technologies, such as biometrics, have also played an important role in the management of refugee flows and in the distribution of humanitarian

aid. However, with heightened security risks which come with the increased incidence of urban warfare, more dangerous and destructive weapons, and an increased number of nonstate actors, the actual protection of civilians caught in conflict is becoming increasingly difficult. The absence of safeguards controlling disinformation, manipulation and data hacking, and lack of agreement of international data and AI standards, further complicates these challenges.

In the short to medium term, guidelines supporting a "minimum basic technology infrastructure" for humanitarian operations and protecting civilians should be agreed upon and developed. The dual-use nature of technology will ensure a continued and spiraling trend where an *illicit* use of a technology becomes used as a potential countermeasure for a *licit* use of a technology. The sluggish progress made on robust data and AI standards, combined with the challenges of harmonizing data standards and data privacy laws transnationally, also weaken the case for an approach based on regulation only. The fact that data-driven and digitalized processes will continue to operate in a predominantly ungoverned cyber domain requires populations to apply effective critical thinking and digital media literacy skills. Guidelines supporting a "minimum basic technology infrastructure" should therefore include an equal focus on technology, regulation, digital literacy and education components.

The evidence reviewed in this article suggests that, based on the current data and technology practices being pursued by both security and humanitarian professionals, the technology component of the infrastructure could build on the current use of GPS, satellite and mobile telephone data. These combined sources of data can be used to analyze the density of civilian populations in need, their movements and the number of people directly impacted by military operations. Such efforts should also consider important issues such as data anonymization and privacy; transparency in data collection; and collaboration between humanitarian and non-humanitarian actors. As the manipulation of information, and a rise in fake news, fake identities and "deep fakes" proliferate social media platforms, partnerships with social media verification analysts capable of augmenting information, and "bunking" and "pre-bunking" narratives, will also provide important capabilities. To protect sensitive data from being manipulated and used against groups and individuals, robust cyber security systems must accompany the required technology, particularly for the protection of verification data generated by biometrics. In the case where other technologies are used for personal identification, humanitarian organizations should continue to be guided by the 1949 Geneva Conventions and their Additional Protocols which form the core of international humanitarian law (IHL) including the Universal Declaration of Human Rights, relevant legislation of the country where such humanitarian activities are carried out, and regional protection regimes and mechanisms (e.g., African Charter on Human and Peoples' Rights, The African Union; and The American Convention on Human Rights, Organization of American States).

Challenges relating to a current lack of international consensus on data suggest that human rights frameworks and international humanitarian law must also adapt to the realities of a data-driven and "intangibles" world. Indeed, achieving international consensus on data use will be predicated on the gradual development of capacity among governments to operate in a this digital environment. At the same time, it is not enough to build the capacity of governments. Public education campaigns focused on enhancing digital and media literacy aimed at a wide range of populations, including those affected by conflict, can also be implemented. These education and awareness programs could be supported by remote training and gaming applications.

This three-pillared guidance (technology, regulation, and digital literacy and education) supporting a "minimum baseline technology infrastructure" for protecting civilians caught in conflict could be developed in collaboration with the UN's Office of the Coordinator for Humanitarian Affairs, leading member states, and the UN's Office of the Secretary-General's Envoy on Technology. This would ensure that the employment of emerging technologies is aligned with existing IHL. It is vital to provide member states with such guidance in order to strengthen the development of domestic measures and legislation compatible with treaty obligations in the face of these new human rights challenges; and support states with the national implementation of the Global Digital Compact (2024) in a manner that supports humanitarian protection and IHL compliance.

The need for systemic change must also acknowledge contemporary data -driven realities of our digital world: a world where progress is only enabled through information supremacy and data rights. This data control and information supremacy requires an 'eco-system' across relevant stakeholders including leading technology providers which are increasingly shaping geopolitics. It should also include security actors whose capabilities can extend to computer protection, data protection, as well as physical protection. This will require a move away from the guarded independence which humanitarian groups have – with good reason – defended for years, but would recognize the fuller scale of cooperation which is necessary for all forms of protection in the information battlespace.

A discussion on the challenges and opportunities brought by the adoption of new technologies should help forge UN-led guidance on a "minimum basic technology infrastructure" to better protect civilians caught in conflict. Such an undertaking requires more than front-facing task forces on AI and roadmaps on digital inclusion; it requires recognition of a wider data and technology "ecosystem," stronger partnerships between humanitarian, technology and security actors, enhanced digital and media literacy capacity, and an international consensus on data and AI governance frameworks.

Author contributions

AF-G: Writing – original draft, Writing – review & editing. JH: Writing – original draft, Writing – review & editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Acland, S., and Willitts-King, B. (2023). Mobile phones for participation: building responsible public-private humanitarian partnerships. Available at: https://blogs.icrc.org/law-and-policy/2023/12/07/mobile-phones-for-participation-building-responsible-public-private-humanitarian-partnerships/.

Adeyeye, A. I., Akinrinde, O. O., and Omodunbi, O. O. (2022). The influence of globalization on insurgency: Boko haram and Al-Shabaab in the age of information technology. *NUST J. Int. Peace Stab.* 5, 15–29. doi: 10.37540/njips.v5i1.119

Anonymous. (2023). *Technology is deepening civilian involvement in war*. De Economist

Anonymous. (2024). *In the economist (London)*. Vol. 451, Number 9402, p. 12). The Economist Intelligence Unit N.A., Incorporated.

Awan, N. (2020). "Mapping trajectories of displacement" in The handbook of displacement. eds. P. Adey, J. C. Bowstead, K. Brickell, V. Desai, M. Dolton and A. Pinkerton (Berlin: Springer International Publishing), 413–429.

CARE International. (2024). *Sudan: a forgotten crisis which the world must pay attention to now.* Available at: https://www.care-international.org/news/sudan-forgotten-crisis-world-must-pay-attention-now.

CBC News. (2023). *How Ukraine is staying connected to the internet — for now*. Available at: https://www.cbc.ca/player/play/video/1.6765098.

CIPESA. (2023). *Sudan conflict affects digital communications and critical service delivery*. Available at: https://cipesa.org/2023/06/sudan-conflict-affects-digital-communications-and-critical-services-delivery/.

Cohen, R. S., Chandler, N., Efron, S., Frederick, B., Han, E., Klein, K., et al. (2020). The future of warfare in 2030: Project overview and conclusions. Santa Monica, CA: RAND Corporation.

Cordesman, A. (2016). *Chinese strategy and military modernization in 2016*. Center for Strategic and International Studies. Available at: https://www.csis.org/analysis/chinese-strategy-and-military-modernization-2016.

Fabian, S. (2021). *Irregular versus conventional warfare: a dichotomous misconception*. Modern War Institute at Westpoint. Available at: https://mwi.westpoint.edu/irregular-versus-conventional-warfare-a-dichotomous-misconception/.

Filipchuk, H. (2021). Digital transformation in Ukraine. Social insurance. *Theory Pract.* 151, 103–118.

FRA. (2019). *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*. European Union Agency for Fundamental Rights. Available at: https://fra.europa.eu/en/publication/2019/data-quality-and-artificial-intelligence-mitigating-bias-and-error-protect.

Hübl, F., Cvetojevic, S., Hochmair, H., and Paulus, G. (2017). Analyzing refugee migration patterns using geo-tagged tweets. *ISPRS Int. J. Geo Inf.* 6:302. doi: 10.3390/ijgi6100302

Human Rights Watch. (2022). *New evidence that biometric data systems imperil afghans, new evidence that biometric data systems imperil afghans*. Human Rights Watch (hrw.org).

Hunder, M., and Balmforth, T. (2024). *Russia pounds Ukrainian power facilities; Zelenskiy seeks air defences, 'political will'*, Reuters. Available at: https://www.reuters.com/world/europe/ukraine-says-russian-strike-hit-ukraines-largest-dam-during-mass-strike-energy-2024-03-22/.

ICRC (2022). Digitalizing the red cross, Red Crescent and Red Crystal Emblems, Benefits, Risks, and Possible Solutions. Geneva: ICRC.

Jacobsen, K. L. (2022). Biometric data flows and unintended consequences of counterterrorism. *Int. Rev. Red Cross* 103, 619–652. doi: 10.1017/S1816383121000928

Joint Publication. (2016). *Unconventional warfare pocket guide, unconventional warfare pocket Guide_v1 0_Final_6 April 2016.Pdf (soc.mil), No. 3-05.1*. Joint Publication.

Joshi, S. (2023). *How Elon Musk's Starlink has changed warfare*. De Economist. Available at: https://www.economist.com/starlink-pod.

Judson, J. (2023). *Change of plans: US Army embraces lessons learned from war in Ukraine*. *Defense News*. Available at: https://www.defensenews.com/land/2023/10/09/change-of-plans-us-army-embraces-lessons-learned-from-war-in-ukraine/.

Kaiser, R., Spiegel, P. B., Henderson, A. K., and Gerber, M. L. (2003). The application of geographic information systems and global positioning Systems in Humanitarian Emergencies: lessons learned, programme implications and future research. *Disasters* 27, 127–140. doi: 10.1111/1467-7717.00224

Kaplan, I. (2018). *How smartphones and social media have revolutionized refugee migration*. UNHCR Blogs. Available at: https://www.unhcr.org/blogs/smartphones-revolutionized-refugee-migration/.

Kilcullen, D. J. (2012). The City as a system: future conflict and urban resilience. *Fletcher Forum World Aff.* 36, 19–39.

Kilcullen, D. (2016). The evolution of unconventional warfare. *Scand. J. Mil. Stud.* 1, 1–18. doi: 10.31374/sjms.3

Kostina, I., and Pohorilov, S. (2024). *Kremlin launches propaganda campaign against France after Macron's statements on Ukraine*. Ukrainska Pravda. Available at: https://www.pravda.com.ua/eng/news/2024/04/4/7449634/.

Larson, E. V. *Assessing irregular warfare*. RAND Corporation (2008). Available at: https://search-ebscohost-com.libproxy.wlu.ca/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=e000xna&AN=276607&site=ehost-live. (Accessed August 29, 2024).

Lavers, C. (2021). *Chris Lavers: space-based monitoring of armed conflict and its impact on civilians*. University of Oxford Blogs. Available at: https://conflictplatform.ox.ac.uk/cccp/research/space-based-monitoring-of-armed-conflict-and-its-impact-on-civilians.

Lichtman, A., and Nair, M. (2015). Humanitarian uses of drones and satellite imagery analysis: the promises and perils. *AMA J. Ethics* 17, 931–937. doi: 10.1001/journalofethics.2015.17.10.stas1-1510

Lyons, J. (2012). Documenting violations of international humanitarian law from space: a critical review of geospatial analysis of satellite imagery during armed conflicts in Gaza (2009), Georgia (2008), and Sri Lanka (2009). *Int. Rev. Red Cross* 94, 739–763. doi: 10.1017/S1816383112000756

Marijan, B. (2023). "*AI guided weapons must be curbed by global rules – and soon*", Centre for International Governance Innovation, AI-guided weapons must be curbed by global rules — and soon - Centre for International Governance Innovation (cigionline.org).

Marks, T. A., and Ucko, D. H. (2023). Counterinsurgency as fad: America's rushed engagement with irregular warfare. *J. Strateg. Stud.* 46, 809–835. doi: 10.1080/01402390.2023.2179616

Metz, S. (2012). The internet, new media, and the evolution of insurgency. *Parameters* 42:3058. doi: 10.55540/0031-1723.3058

MOAS. (n.d.) Available at: https://www.moas.eu/.

OCHA. (2023a). *Global humanitarian overview*. Available at: https://2022.gho.unocha.org/delivering-better/towards-enhanced-data-responsibility-humanitarian-action/.

OCHA. (2023b). *OCHA's strategic plan 2023-2026: transforming humanitarian coordination*. Available at: https://www.unocha.org/publications/report/world/ochas-strategic-plan-2023-2026-transforming-humanitarian-coordination.

Poole, D. N., Raymond, N. A., and Khoshnood, K. (2023). Satellite imagery identifies deliberate attacks on hospitals. *Nature* 618:30. doi: 10.1038/d41586-023-01759-7

Quintana, G. (2023). *Space Technology in Humanitarian aid: mapping crises and enhancing response*. Groundstation. Available at: https://www.groundstation.space/tech/space-technology-in-humanitarian-aid-mapping-crises-and-enhancing-response/.

Rabasa, A., Gordon, J., Chalk, P., Grant, A. K., McMahon, K. S., Pezard, S., et al. (2011). "From insurgency to stability" in Volume II: Insights from selected case studies (Santa Monica, CA: RAND Corporation).

ReliefWeb. (2023). *Addressing the impact of Mis-/disinformation on civilians, addressing the impact of Mis-/disinformation on civilians – world*. ReliefWeb.

Schwarz, E. (2024). *The Gaza war: Israel using AI to identify human targets raising fears that innocents are being caught in the net", the conversation*. Available at: https://theconversation.com/gaza-war-israel-using-ai-to-identify-human-targets-raising-fears-that-innocents-are-being-caught-in-the-net-227422.

Smith, T. W. (2008). Protecting civilians…or soldiers? Humanitarian law and the economy of risk in Iraq. *Int. Stud. Perspect.* 9, 144–164. doi: 10.1111/j.1528-3585.2008.00324.x

Trusilo, D., and Danks, D. (2023). Artificial intelligence and humanitarian obligations. *Ethics Inf. Technol.* 25, 1–5. doi: 10.1007/s10676-023-09681-2

UN Women. (2024). *Placing gender equality at the heart of the global digital compact: taking forward the recommendations of the sixty seventh session of the commission on the status of Women*. Available at: https://www.unwomen.org/en/digital-library/publications/2024/03/placing-gender-equality-at-the-heart-of-the-global-digital-compact.

UNHCR. (2016). *The Office of the United Nations High Commissioner for refugees global strategy on connectivity for refugees*. Available at: www.unhcr.org/innovation/connectivity-for-refugees.

UNSG. (2021). *Our common agenda – Report of the secretary-general*. Available at: https://unglobalaccelerator.org/resource/united-nations-secretary-generals-report-our-

common-agenda#:~:text=The%20Our%20Common%20Agenda%20report,access%20the%20Common%20Agenda%20here.

Wise, P. H., Shiel, A., Southard, N., Bendavid, E., Welsh, J., Stedman, S., et al. (2021). The political and security dimensions of the humanitarian health response to violent conflict. *Lancet (London, England)* 397, 511–521. doi: 10.1016/S0140-6736(21)00130-6

Zeitzoff, T. (2017). How social media is changing conflict. *J. Confl. Resolut.* 61, 1970–1991. doi: 10.1177/0022002717721392

Zhou, W. (2023). *War, law and outer space: pathways to reduce the human cost of military space operations.* Humanitarian Law and Policy. Available at: https://blogs.icrc.org/law-and-policy/2023/08/15/war-law-outer-space-reduce-human-cost-of-military-space-operations/.