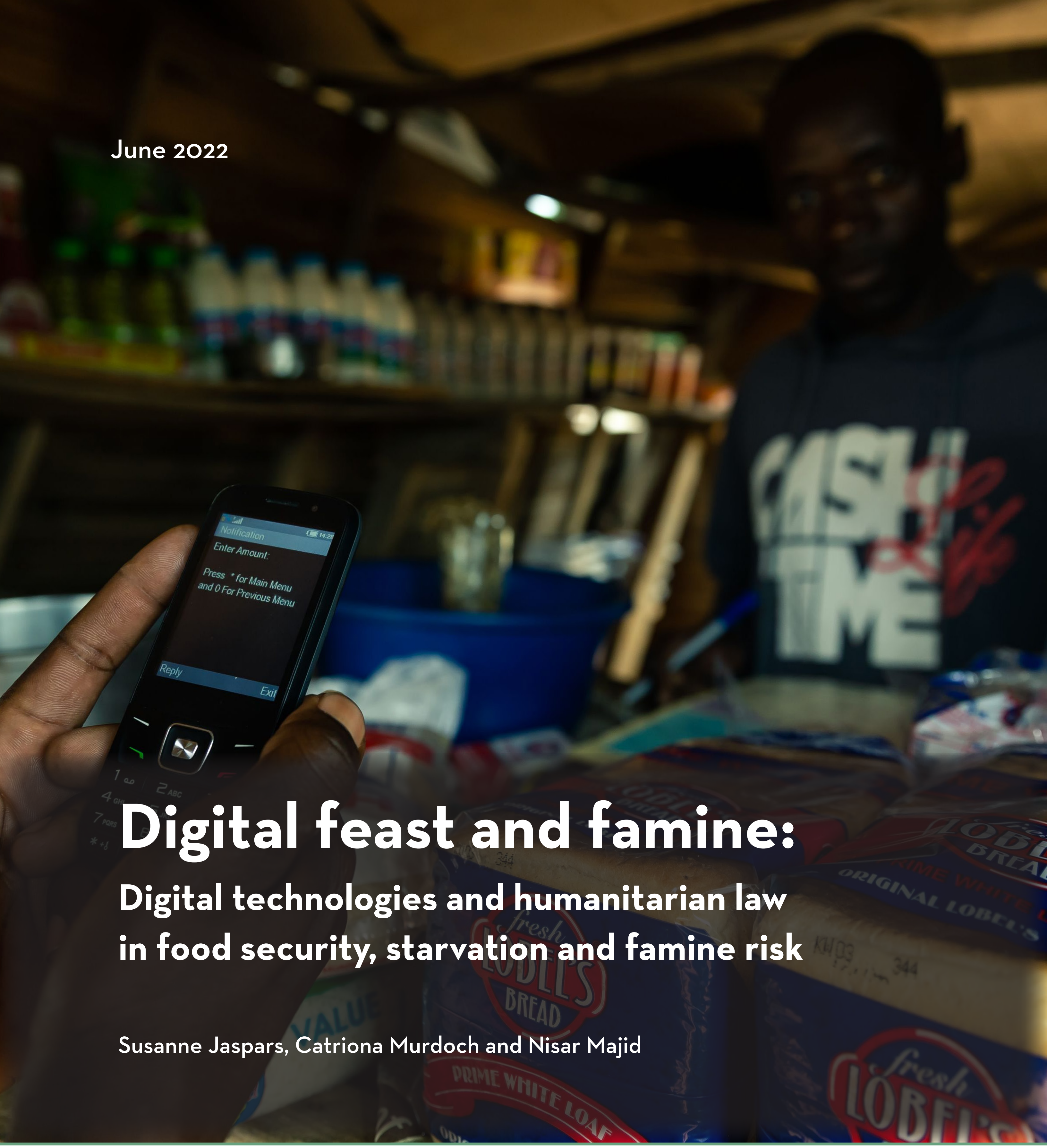

June 2022

Digital feast and famine:

Digital technologies and humanitarian law in food security, starvation and famine risk

Susanne Jaspars, Catriona Murdoch and Nisar Majid

WORLD PEACE FOUNDATION

LSE Ideas

PeaceRep
Peace and Conflict
Resolution Evidence
Platform

ABOUT

This research is supported by the Peace and Conflict Resolution Evidence Platform (PeaceRep), funded by UK Aid from the UK Foreign, Commonwealth & Development Office (FCDO) for the benefit of developing countries. The information and views set out in this publication are those of the authors. Nothing herein constitutes the views of FCDO. Any use of this work should acknowledge the authors and the Peace and Conflict Resolution Evidence Platform.

PeaceRep: The Peace and Conflict Resolution Evidence Platform is a research consortium based at Edinburgh Law School. Our research is rethinking peace and transition processes in the light of changing conflict dynamics, changing demands of inclusion, and changes in patterns of global intervention in conflict and peace/mediation/transition management processes. PeaceRep is funded by the Foreign, Commonwealth and Development Office (FCDO) UK. Our partners include Austrian Study Centre for Peace and Conflict Resolution, Conciliation Resources, Edinburgh Centre for Constitutional Law, International IDEA, LSE IDEAS, LSE Middle East Centre, Queens University Belfast, University of St Andrews, and the University of Glasgow.

University of Edinburgh, School of Law, Old College, South Bridge, EH8 9YL
PeaceRep.org | @Peace_Rep_ peacerep@ed.ac.uk

The World Peace Foundation: World Peace Foundation, an operating foundation affiliated solely with the Fletcher School at Tufts University, aims to provide intellectual leadership on issues of peace, justice and security. We believe that innovative research and teaching are critical to the challenges of making peace around the world, and should go hand-in-hand with advocacy and practical engagement with the toughest issues. To respond to organized violence today, we not only need new instruments and tools—we need a new vision of peace.

World Peace Foundation at The Fletcher School of Law and Diplomacy, Tufts University
169 Holland Street, Somerville, MA 02144
worldpeacefoundation.org | @WorldPeaceFdtn

AUTHORS

Susanne Jaspars is an independent researcher and a research associate at LSE and at the Food Studies Centre, SOAS, University of London. She has more than 30 years' experience of research and operational work in the social and political aspects of food security, livelihoods, and humanitarian aid in situations of famine, conflict and humanitarian crisis. Her regional expertise is mainly in the Horn and East Africa, in particular Sudan and Somalia. She recently completed a PhD on the history and politics of food aid in Sudan. Susanne has published a number of books, articles and policy reports, including *Food Aid in Sudan: a History of Power, Politics and Profit* (Zed Books, 2018).

Catriona Murdoch is an international criminal and human rights lawyer, with expertise in the crime of starvation, associated starvation violations and right to food abuses. She has a granular knowledge of conflict and hunger across Yemen, Syria, South Sudan and Tigray. Called to the Bar of England and Wales and attached to 1 Crown Office Row Chambers in the UK, Catriona leads GRC's Starvation Portfolio, and also supports various GRC projects, notably the DPRK Accountability Project. Catriona pioneered the Starvation Training Manual and leads training to a range of beneficiaries. Catriona has practiced international criminal law for over 13 years, advising on crimes arising out of the Rwandan Genocide, the Iraq war, the current conflicts in Yemen and the war in the former Yugoslavia.

Nisar Majid is an independent researcher and research associate at the LSE. He was Research Director on the LSE Conflict Research Programme (Somalia), 2018-2021. He has worked on Somali-related issues since the late 1990s in a variety of applied research capacities. His early work was in food security and livelihoods analysis, while his later doctoral research explored the transnational engagement of the Somali diaspora across the Somali regions of the Horn of Africa. He has led and/or participated in numerous reviews and evaluations in the region and has worked closely with a wide variety of international agencies. He is co-author of the book, *Famine in Somalia: Competing Imperatives, Collective Failure, 2011-2012* (Hurst, 2016).

Cover Photo: Jekesai Njikizana\Getty Images

ACKNOWLEDGEMENTS

Many people helped in completing this study. First, we would like to thank Alex de Waal and Fiona Terry for being on our advisory group. They helped us think through the issues and reviewed draft notes and reports. We would also like to thank others who reviewed the draft report: Christine Bell, Rebecca Sutton, Emanuela-Chiara Gillard, Kristin Bergtora-Sandvik, Pierrick Devidal, Deborah Baglole, Nick Leader and Dan Maxwell. Many more people gave their time to be interviewed and to tell us the key issues in their country and/or helped us learn from their expertise. Thank you!

TABLE OF CONTENTS

EXECUTIVE SUMMARY

> **Now if you cut the internet and phone networks, people are lost. It becomes as if you are cutting off their source of life.**
>
> *Aid worker in Sudan, March 2022*

This working paper presents the findings of **a brief exploratory study into the role of digital technologies in International Humanitarian Law (IHL) and its implications for starvation and famine risk.** It is a work in progress, intended to raise issues rather than reach definitive conclusions (given the short timeframe). As a work in progress it seeks to elicit comments and generate discussion about the advantages and risks of digital technologies in situations of conflict and famine, between (and within) practitioners and policy-makers and lay the groundwork for further exploration and research. It is based on a literature review, and a limited number of (remote) interviews (33), mostly done during the month of March 2022.

The last decade has seen **a return of famine and an increase in weaponised starvation**, largely linked to conflict. The war in Ukraine, because it has disrupted global supplies of wheat, fertilizer, and fuel, has added another layer to what was already becoming a severe global food crisis. Over the same time period, **food security, food systems and humanitarian response have become increasingly digitalised,** including mobile phone and internet to communicate, assess, analyse (machine learning) and transfer money (debit cards, banks, mobile money), as well as digitalised biometrics and beneficiary identities. **Cyberoperations are increasingly used in war** to disrupt or shutdown networks, and we explore whether and how the prohibition of starving civilians under IHL applies. This paper is a first exploration on what the important issues are for digital technologies and humanitarian law in food security, famine and starvation risk (see Box 1 for definitions).

In conflict situations, **warring parties can manipulate social media and shutdown mobile phone and internet connections,** which has serious implications for the severity of conflict, food systems and livelihoods. Social media spreads disinformation about opposition forces, the nature of conflict, or about humanitarian organisation or actors, all of which can fuel conflict or disrupt aid. Network shutdowns are usually intended to prevent enemy forces, or protestors, from organising, or to prevent news coming out. From our findings, it has also had the effect of blocking aid, stopping financial transfers (including remittances), stopping banks functioning, closing shops and trade, and inhibiting IDPs from accessing security information to move, e.g. for farm work. This was more evident in Sudan, Ethiopia and Somalia, than in Syria and Yemen where digital technologies for remittances, financial transfers, or aid, are not prevalent to start with (for external reasons of sanctions, and internal ones of suspicion and control).

Examining a population's dependence on digital technologies and the possibility for political actors to interfere with it or shut it down is an important consideration as part of a more comprehensive famine analysis. The majority legal opinion is that IHL applies to cyberoperations, and that under certain circumstances digital infrastructure (and possibly their functioning) can be considered items indispensable to survival (OIS) that are protected. On-the-ground empirical evidence is needed.

As digital technologies proliferate, humanitarian and human rights organisations use them to assess food security, famine risk and starvation crimes. Monitoring food security has become increasingly quantitative in recent years, which is conducive to remote and digital assessments for hard to access conflict-affected populations. While this has some advantage for access and speed, there are limitations in terms of exclusions (where connectivity or mobile phone ownership is limited) and for understanding the complexities of famine causation. Similarly, artificial intelligence (AI) has been used for Famine Early Warning, but does not include the political choices which often cause famine and determine response. In contrast, the recent focus on famine crimes is precisely to put the politics back into famine analysis, with UN Security Council resolution (2417) framing the issue and reiterating that starvation of civilians is prohibited and may amount to a war crime. **Famine researchers and legal experts have used digital forensics as part of investigations into famine crimes.** Digital technologies have harnessed open-source intelligence and information (OSINT) including geolocation, visual analysis, geospatial data including heat maps and fire data, to social media intelligence (SOCMINT), crisis mapping as well as those used for food security and market monitoring. In determining causality and intent, these are usually combined with field investigations and/or interviews with human rights monitors, witnesses or survivors. Once reliable information is obtained a range of procedures exist to use it before justice and accountability mechanisms, including courts.

Digital humanitarian aid also needs to be considered in terms of **access, potential risks (the protection of civilians) and humanitarian principles.** The potential risks and exclusions associated with digital assistance are likely to affect politically marginalised populations the most. As they are already the most vulnerable to famine, it can lead to increased inequality and vulnerability. In addition to exclusions due to limited connectivity, lack of national ID cards is source of exclusion, particularly for migrants and displaced populations. The digital aid discussed in this paper is particularly cash transfers, including biometric identification systems, bank cards and ATMs, or mobile money. Mostly these can be blocked in situations of war, just like material aid can be.

A key risk in digitalised assistance is politically motivated exclusions or persecution based on centralised digital beneficiary identification systems. In fact, whether civilian data are a protected object under IHL is a topic debated by international legal experts. This also links to the issue of cyberattacks on the computer systems of humanitarian organisations (or of data held by private data management or technology companies), and their potential to be violations of IHL. **Extensive private sector involvement also raises an issue about the impartiality, neutrality and independence** of humanitarian relief (a requirement under IHL). Although not directly related to famine, private sector interests are rarely compatible with humanitarian concerns. Instead, interests are likely to be profit thus feeding into the inequalities that contributed to famine in the first place.

With the current increasingly severe global food crisis, the use of digital technologies to assess, monitor and respond to the crisis will no doubt proliferate. This makes it all the more important to continue to examine their role in famine and starvation: fuelling conflict (social media disinformation), vulnerability/power (dependence on technology, risk of exclusions and increased inequality), information and access, protection (of data and people), and how international humanitarian law can be used.

1. Introduction

The aim of this paper is to explore the role of digital technologies in the violation and application of humanitarian law, and its consequences for famine risk and prevention. The last decade has seen a return of severe famine and mass starvation (De Waal, 2018), and at the same time a digitalisation of food security and famine response. As current famines are mostly conflict-related, and digital technologies have also become part of the way in which war is fought, the adoption of these technologies raises issues with regard to International Humanitarian Law (IHL) or rather the rules of war and the protection of civilians.

Recent studies have looked at the role of international law in conflict-induced food insecurity and in promoting accountability for mass starvation (see for example:Jordash et al., 2019, Akande and Emanuela-Chiara, 2019). The role of digital technologies in humanitarian law is also beginning to be explored (Rejali and Heiniger, 2020), as is the effect of digitalising humanitarian and food assistance in attempting to meet needs more effectively (Sandvik et al., 2014, Jaspars and Sathyamala, 2021). However, the link between famine, digital technologies and humanitarian law has not been studied before. This paper is a first exploration of what the key issues are, in terms of the role of digital technologies in food security and famine risk, the application of IHL, and what it means for analysis and action in conflict-induced humanitarian crises. The anticipated audience are humanitarian practitioners, governmental and policy stakeholders, who will hopefully be able to use the findings to help examine benefits and risks of using digital technologies in conflict settings and determine what information is needed for decision-making. The report also identifies a number of areas for more in-depth on-the-ground research.

The paper starts with a section on key concepts and definitions in famine, IHL and digital technologies. The section that follows explores how warring parties may manipulate or undermine mobile phone and internet networks, the impact on food security and famine, and how this is – or can be – considered in international law. Section 4 looks at how digital technologies can help to assess and analyse famine and starvation crimes. Finally, we explore the use of digital technologies in food assistance responses, in particular cash transfers, and the advantages and risks they pose for civilians in terms of their vulnerability to famine. Key aspects include access to civilian populations, humanitarian principles, and protection. The conclusion covers key issues for consideration in the use of digital technologies in situations of conflict and humanitarian assistance, for famine prevention – legal and operational – and what needs to be explored further.

2. Famine, IHL and digital technologies: concepts, definitions, and methods

As of early 2022, twenty countries are predicted to experience food crisis or famine (FAO and WFP, 2022), reflecting a trend of increasing famine and mass starvation over the past decade (De Waal 2018). Other reports place the number of countries in acute food insecurity at 53 (Global Network Against Food Crisis, 2022). The rise in global wheat and fuel prices resulting from war-disrupted production in Ukraine and Russia, alongside a naval blockade of Ukraine's Black Sea ports, adds another risk, as countries like Sudan, Somalia and Yemen are highly dependent on imports (Maxwell, 2022). This section starts with an overview of famine and how it links to starvation as a violation of international law. It then looks at the prohibition of starvation in IHL, and the use of digital technologies in food security and famine response. From there it outlines the objectives and methods of this study.

Famine has multiple causes (international, national and local), including power relations and political decisions, social and economic processes, and involves large numbers of people not being able to access sufficient food for survival. Now, as in the past, conflict and violence causes the most severe famines (De Waal, 2018), often in historically marginalised groups who already experience protracted crisis. Marginalised groups, for example in Somalia and Sudan, have been politically under-represented and often subjected to land-grabs, attacks, displacement and exploitation. Powerful elites dominate trade and business – and are able to manipulate markets to their own advantage. Aid has often become part of this political economy (Maxwell and Majid, 2016, Jaspars, 2018, Jaspars et al., 2020). Famine definitions have ranged from a focus on large numbers of people experiencing a collapse in food entitlements (or access to food), starvation and death (Sen, 1981), to social disruption, destitution and disease (De Waal, 1989) (see Box 1). While causes are now acknowledged to be largely political in nature (Devereux, 2007), famine identification has become highly technical with the adoption of the Integrated Phase Classification (IPC) system[1] for classifying food insecurity using thresholds for quantitative indicators of malnutrition, mortality and food insecurity (this is further discussed in section 4).

War causes famine through specific acts that undermine the means of livelihood or survival of particular population groups. Macrae and Zwi (1994) have classified these as acts of commission, omission and provision. Acts of commission include attacks on production, markets and the restriction of access for humanitarian actors, or the obstruction of relief, amongst other acts. Acts of omission include failures to act in response to warnings or signs of famine, and acts of provision the selective provision of food to one side of the conflict. These tactics can be part of counter-insurgency operations but also provide benefits to business by raising food prices and often lowering livestock or labour costs with distress sales and migration (Keen, 1994). The return of extreme famines from 2007 onwards can in part be attributed to political acts (or inaction) not only on the part of governments nationally, but also internationally as political priorities and national security increasingly trump humanitarian concerns (for example in the War on Terror, or with priorities of stemming migration to Europe) (De Waal, 2018).

Famine as the result of political decisions and power relations highlights the need to understand how **acts of starvation** were committed and by whom (Edkins, 2007; De Waal 2018). For this reason, De Waal (2018: 6) argues that 'we must include *forced mass starvation* in definitions of famine and regard it as a variant of mass atrocities'. It also means that raising awareness of the crime of starvation and holding those who cause deliberate starvation to account, can be part of famine prevention (De Waal, 2018; GRC and WPF, 2019). Intentionally starving civilian populations is prohibited under **International Humanitarian law (IHL) and International Criminal Law (ICL).** Its prohibition is irrespective of the international or non-international character of the armed conflict in question. In IHL, pursuant to Article 54(2) of Additional Protocol I of the Geneva Conventions:

> It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population […] for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive.

Its counterpart in non-international armed conflict (NIAC) has the same prohibition.[2] The term 'rendering useless' as found in the IHL and ICL definitions of the prohibition of starvation, has been interpreted to include a flexible range of operations, not limited to kinetic attacks or destruction (Gisel et al., 2020) and thus including cyber operations (this is further discussed in section 3.2). The prohibition of starvation has also gained the customary law status,[3] and includes denying access of

[1] http://www.ipcinfo.org/ipc-manual-interactive/en/

[2] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, 1125 UNTS 609

[3] Customary law is a set of rules derived from consistent conduct of States ('state practice') acting out of the genuine belief that the law –

humanitarian aid intended for civilians in need (Akande, D. and G. Emanuela-Chiara, 2019; GRC, 2022). The regulation of humanitarian assistance under IHL, is a related but separate issue from the prohibition of starvation. Under IHL, parties to an armed conflict have an obligation to allow and facilitate the rapid and unimpeded passage of humanitarian relief (subject to the relief being impartial, conducted without any adverse distinction, and subject to the parties' right of control).[4] When a civilian population faces the threat of starvation, the warring party must accept the offer of impartial relief to alleviate that suffering, with consent only being withheld for 'valid and compelling reasons' (GRC, 2022, Sandoz et al. (1987): 4876-4885, ICRC, 2014: 11, Bothe, 2013: 485).

The term "objects indispensable to survival" (OIS) found in IHL and ICL includes objects broader than just food, encompassing water installations and supplies, irrigation works, medicine, clothing, shelter, fuel and electricity (Triffterer and Ambos, 2016). At its core, the prohibition to attack, destroy or render useless OIS, reinforces the fundamental principles of IHL, namely distinction between civilians and combatants and between civilian and military objects (see section 3.2); proportionality; and military necessity.[5] The means to sustain life and the term OIS are likely to be interpreted broadly in a legal sense and are not subject to a pre-defined list (GRC and Mwatana for Human Rights, 2021).

The war crime of starvation under the International Criminal Court's Rome Statute mirrors the IHL prohibition, and outlines two essential elements that are required to establish the offence (in addition to the two chapeau elements necessary for the war crime[6]): (i) the perpetrator deprived civilians of OIS; (ii) the perpetrator intended to starve civilians as a method of warfare. The war crime offers the illustrative example of wilfully obstructing humanitarian aid as the means with which the crime may be committed. Most recently, in 2018, the UN Security Council unanimously adopted resolution 2417 which condemns the use of starvation as a method of warfare against civilians and emphasised that the use of starvation of civilians as a method of warfare may constitute a war crime.

Digital technologies are part of most people's lives, and as such are part of food systems, war strategies, and humanitarian assistance. These technologies have proliferated in the past two decades with a surge in technocratic approaches following the 2008 food and finance crisis, and with the recent Covid-19 pandemic, as a way of socially-distanced or remote working (Jaspars and Sathyamala, 2021). For the same reason, they play a role in food security, famine, and response. Digital technologies include a wide range of practices, such as the use of mobile phone and internet networks to communicate, assess, and transfer money, the use of biometrics for identification, debit cards and banking, and the use artificial intelligence to categorise and predict need. Many countries are digitalising their food systems – to manage production and delivery, and to provide information and services to farmers and traders (Bahn et al., 2021). In countries currently at risk of famine, however, technologies in food systems are more likely to be mobile phone and internet networks, rather than

Digital technologies are part of most people's lives, and as such are part of food systems, war strategies, and humanitarian assistance.

as opposed to, e.g., courtesy or political advantages – required them to act that way ('opinio juris'). International Court of Justice ('ICJ'), North Sea Continental Shelf Cases (Germany/Denmark, Germany/Netherlands), Judgment, 20 February 1969, paras 71-74, 77. See also Sassòli (2019: 46).

[4] GC IV, Articles 23, 59, 61, AP I, Article 70; AP II, Article 18(2), Customary IHL, Rules 55-56

[5] Proportionality. Parties to the conflict may not launch an attack on military objectives if it will result in excessive civilian deaths. Precaution. Take all measures to protect the civilian population. Military necessity permits measures which are essential for securing the end of the war and which are lawful under IHL. *Katanga* Trial Judgment, para. 894.

[6] The two chapeau elements necessary for the war crime are (i) the conduct took place in and was associated with an international armed conflict (ii) the perpetrator was aware of factual circumstances that established the existence of an armed conflict.

computational or predictive analytics, GPS and satellite imagery, robotics, or blockchain.[7] In conflict situations, little or nothing is known about how digital technologies are used in agriculture (ibid.: 19). In aid, digital technologies are used in assessment, early warning, and response. Assessments may use mobile phones, social media platforms and satellite imagery, and AI for early warning. In response, the use of biometrics (iris scans or fingerprints), smart cards and banking, or the transfer of money direct through mobile phones are now common (Duffield, 2018, Bryant et al., 2020, Hamilton, 2021, Jaspars and Sathyamala, 2021).

The study explores the potential role digital technologies may play in relation to two facets of conflict which feature starvation as a result of violations of International Humanitarian Law (IHL) (Jordash et al. 2019; Akande and Emanuela-Chiara 2019). First, the deprivation OIS of the civilian population, which includes an analysis of the ways digital technologies are used in food systems in conflict contexts. The paper focusses particularly on the nature and effect of shutting down internet and mobile phone networks, which we argue can meet the everyday definition of OIS in some situations. Second, we examine digital technologies in relation to the obligation to provide unimpeded access to humanitarian aid. In addition, we examine in brief the risks to the protection of civilian populations that digital technologies themselves pose and the implications for humanitarian principles (i.e., humanity, neutrality, impartiality and independence).

Methods for this exploratory study included a brief review of the literature on digital technologies, humanitarian law and/or humanitarian action and food security, and on the relevant legal instruments. We also conducted 9 interviews with key informants with general knowledge of digitalisation and humanitarianism (academics and regional or headquarter organisational representatives) and gathered slightly more detailed information on Sudan, Ethiopia (Tigray), Somalia, Yemen, and Syria (including 24 interviews or discussions to gather information on different environments in terms of the nature of conflict, governance, and dependence and availability of mobile networks). The aim of these interviews was to gain an understanding of the key issues and to guide the literature review, and to get an initial impression of on-the ground evidence of impact of digital technologies on famine risk. These interviews took place mostly in March 2022 (with a limited number in April and May) and were done remotely.

[7] Blockchain is a distributed ledger technology in which accounts of information or transactions are maintained across several computing devices and linked to a peer-to-peer network. It is said to be a secure way of storing data or to conduct financial transactions, overcoming potentially corrupt authorities or poorly functioning banking systems (Coppi and Fast, 2019).

BOX 1 – Definitions of famine, starvation and humanitarian law

Starvation covers the processes of deprivation that occur when actors impede the capacity of targeted persons to access the means of sustaining life. Attacking, destroying or rendering useless objects indispensable to survival (OIS) is clearly prohibited in international law. OIS include objects broader than just food, encompassing water (including water installations, supplies and irrigation works, medicine, clothing, shelter, fuel and electricity (Triffterer and Ambos, 2016: 513)

Famine has several definitions, all of which include restricted access and availability to food, and some include social disruption (including distress migration), malnutrition and death for a large proportion of the population. The Integrated Food Phase Classification (IPC) System identifies famine when 'households have an extreme lack of food and/or other basic needs even after full employment of coping strategies' (20% or more of the population); and where conditions of starvation, death, destitution, and extremely critical acute malnutrition levels (>30%) and mortality (>2/10,000/day) are evident (IPC Global Partners, 2021).

Food security Food security exists when all people, at all times, have physical, social and economic access to sufficient, safe and nutritious food to meet their dietary needs and food preferences for an active and healthy life. The four pillars of food security are availability, access, utilization and stability. The nutritional dimension is integral to the concept of food security (FAO, 2009).

International Humanitarian Law (IHL) is a set of rules that seeks, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not, or are no longer, directly or actively participating in hostilities, and imposes limits on the means and methods of warfare. IHL is also known as "the law of war" or "the law of armed conflict". IHL is part of public international law, which is made up primarily of treaties, customary international law and general principles of law (see Article 38 of the Statute of the International Court of Justice).

International Criminal Law is the part of public international law that deals with the criminal responsibility of individuals for the international crimes of war crimes, crimes against humanity, genocide, and aggression (The Peace Palace Library).[8]

Cyberwarfare and cyberoperations are generally understood as digital attacks on an enemy's computing systems or networks which can cause injury, death or destruction (including of critical infrastructure, such as electricity, health care, water supplies or food logistics) (Ranger, 2018, ICRC, 2021). Cyberoperations, according to ICRC, may also include '… , the interruption, deception or obfuscation of the enemy's communication systems aimed at hindering force coordination; … ' (Gisel et al., 2020: 291).

[8] https://peacepalacelibrary.nl/

3. Undermining digital infrastructure and the risk of starvation

In today's wars, digital technologies can be used to disrupt critical infrastructure (water, food, electricity, banks); mobile phone and internet networks can be shut down thus hiding information on the extent of crisis[9] as well as interrupting social networks, money transfers, and more. Social media accounts can be targeted and manipulated, fuelling political and societal division and polarisation. This section first examines these issues for countries at risk of famine, in particular what happens if networks are manipulated or shutdown, followed by a reflection on the legal aspects of such shutdowns in relation to IHL.

3.1 Digital technologies in livelihoods and food systems and the effect of shutdowns

Internet and mobile phone networks have become an essential part of life for many populations; to maintain social networks, to share information on security or, as part of food systems, on production, markets and trade, and to transfer money. This section discusses to what extent people are dependent on digital technologies for their livelihoods, and therefore their vulnerability to manipulation and shutdowns or network disruptions,[10] and how it varies in different contexts. As discussed below, key variations appear to be in the number of network providers, how reliable they are, mobile phone and internet usage, and the extent of government control (or by other authorities).

Spreading disinformation

Social media (facebook, twitter, instagram) spreads **misinformation, disinformation, and hate speech (MDH),** and thereby creates and amplifies existing divisions within society. As such, social media has been associated with exacerbating conflict, potentially contributing to famine risk and starvation crimes. Social media has been used to promote certain narratives about the conflict and about who is responsible for humanitarian or economic consequences. This can include the use of 'deep fake'[11] images or videos the use of which is suspected in the war with Ukraine (Diepeveen et al., 2022). Social media has also been used by activists to organise protests (perhaps against a government's political choices, war strategies or economic mismanagement), and governments or warring parties may try to block this.

Disinformation may fuel conflict by providing misleading information or propaganda on the "enemy" and its perceived supporters. In South Sudan, in 2017, online hate speech was thought to be a key factor increasing the severity of conflict: with inflammatory rhetoric and stereotyping of particular ethnic groups on social media leading to targeted killings and rape, according to the UN Special Advisor on Prevention of Genocide (Reeves, 2017). Before this, social media content had presented the conflict as due to ethnic differences rather than about political power thus misinforming about causes and leading to actual inter-ethnic division (Cosmas, 2014). To a lesser extent in Darfur, according to one interviewee, pictures of violence and destruction on social media have been used to draw people into the conflict. Disinformation can spread by states or other warring parties, and control of networks appears to be an important factor. In Yemen, tight control over social media (and all digital technology) by the Houthi means they use it to control the narrative about the causes of conflict and the population's suffering – putting the blame on the Saudi coalition and their US backers. According to Muggah (2022) a parallel war in Yemen is playing out in cyberspace, with social media access in Houthi areas limited to

[9] It can also be argued that shutting down phone and internet networks can also draw attention and generate more interest by journalists, human rights organisations and others to find out what is happening.

[10] This can include: controlling, jamming, slowing down certain websites and hacking private accounts, as done for example by Sudan's National Intelligence and Security Services (Ali, 2021). Non-functioning or interruptions of electricity networks also affects communications as people cannot charge their mobile phones.

[11] The creation of fake images or videos using artificial intelligence and machine learning.

pro-Houthi platforms, as part of general strategy of media control and campaigns against Saudi attacks and US airstrikes.[12] With separate and highly-controlled internet providers in Houthi areas and those controlled by the Internationally Recognised Government (IRG) in Aden, people living in each area have a very different picture of the war (and of what is true). The spread of disinformation has also led to attacks on particular social groupings (ibid.). Similarly in Somalia, Al-Shabaab, an Islamist group in control of much of rural southern and central areas, forbids the use of smartphones in their area as a means of control.

In Ethiopia, the government has used an aggressive strategy to control information about the war in Tigray. It started with journalists being arrested, followed by a complete communications blackout thus effectively banning communication about the crisis (African Arguments, 2022). Active disinformation through social media consisted of accusations that the Director of WHO was procuring arms for Tigrayan forces, and recasting the war as a struggle between Abiy's regime and neo-colonialists. It also included accusing humanitarian organisations of spreading misinformation and siding with the Tigrayans. The disinformation was used to suspend two organisations (Ahmed, 2021, African Arguments, 2022). States may also accuse journalists and aid workers of spreading fake news, and in some cases, for example Sudan, can accuse service providers of violating the law and restrict them accordingly (Ali, 2021: 115). Also in Sudan, interference with the social media accounts of activists has recently been reported (Radio Dabanga, 2022). An important point is here is that tech-savvy activists are fighting back. Young Yemenis are findings ways to get onto Instagram, Twitter, and TikTok to advocate for more attention to the crisis (Muggah, 2022). Similarly in Sudan, young activists found ways of maintaining contact with the outside world (via Virtual Private Networks) in some shutdowns since the revolution from December 2018 onwards (Ali, 2021), sometimes with help from telecoms engineers (Moore, 2020).

Social media can amplify division and hatred and increase the severity of conflict, thus potentially leading to famine and starvation. The specifics of whether and how the hatred and division leads to starvation crimes or famine needs further exploration; i.e. how does it lead to the destruction of objects indispensable to the survival of particular population groups? What are the humanitarian consequences in terms of access to food, water, health care, etc.? How does it exacerbate existing humanitarian needs? It needs to be born in mind that rather than creating new causes of famine or starvation acts, social media has the potential to magnify already existing social and political tensions or add to existing tactics of disinformation and propaganda in situations of war (ICRC, 2020). Although there are past examples where information can cause harm, social media can increase the scale, speed and impact of information on different audiences (ibid.: 29). Determining famine risk needs to remain grounded in an analysis of the social, political and economic processes that cause it, and how social media can feed into this.

Network shutdowns

Cyber operations may interrupt the functioning of mobile phone and internet networks which impact on food systems and livelihoods by blocking or disrupting communication, separate from its possible effect on computer systems that are essential to the functioning of critical infrastructure (see Box 1 for definitions). As the remainder of this section shows, network shutdowns, even when intended to hinder force (or protestor) coordination, or to prevent news from coming out, can also create starvation or famine risks.

In our interviews, we found three effects that potentially link network shutdowns to starvation. First, **blocking communications networks hides information** on violations of human rights and humanitarian law – and 'invisibilises famine' (as suggested by one of our interviewees) and its causes. Denying

[12] Houthi control the .ye domain, which can be used instead of .com, and control the local internet service provider. The government in Aden has its own internet provider. Only tech-savvy Yemenis can get access to Virtual Private Networks and escape the control and surveillance (Muggah, 2022).

famine or making famine invisible is nothing new – governments have attempted this in many past famines (including in Sudan and Ethiopia) but blocking digital communication systems to prevent information coming out is a new way of doing so. This can be particularly effective when only few network providers exist and/or if they have close links to government as a warring party.

Second, **the possibility of blocking aid with network shutdowns**. In Tigray, where the Ethiopian government has imposed a complete communications black-out for over a year, journalists and aid organisations have suggested that this is also a de-facto aid blockade, as aid organisations have faced extreme difficulties in being able to operate, deliver aid or conduct any form of assessment of humanitarian need (Al-Jazeera, 2022). Humanitarian action has been severely hampered by a lack telecommunication services as well as fuel, banking services, and electricity (Mulford 2021). Ethiopia's flagship social protection programme (PSNP) could be stopped in Tigray early in the conflict, as it was centrally managed by the federal government in Addis Ababa and it was dependent on mobile money or banks (WPF, 2021, GSMA, 2021a, GSMA, 2021b). Digital humanitarian cash transfers were already limited (GSMA, 2021a). In Sudan, where digital cash transfers have been implemented in some parts of the country, the shutdowns following the coup meant (according to one interviewee) that they had to postpone assistance as communication on registration was not possible and banks were not functioning.

Third, network shutdowns also have serious implications in terms of depriving people of OIS, because they **disrupt social networks, food systems and undermine livelihoods.** Social networks are vital in preventing famine, as they link crisis-affected populations to relatives in urban areas or part of the diaspora who can provide support (see for example Maxwell and Majid 2016). In Tigray, a large diaspora normally supports family back home with financial transfers but only sporadic and informal transfers have been possible during the communications blackout. Furthermore, with banking services blocked due to internet shutdowns, people are unable to access their savings (the TPLF-led government had encouraged people to keep their savings in the bank) and small businesses are unable to operate (Gebremichael, 2022, WPF, 2021). In Sudan, similar issues of blocking access to vital resources were reported, although shutdowns have not been as long. In 2019, in the first part of the revolution, the Transitional Military Council shut down communications on a number of occasions (Ali 2021), but the longest was a period of almost a month following the October 2021 military coup. The primary goal was to stop activists organising protests and hiding information about violence against protestors but it also meant that money transfers could not take place and banks and shops could not function. The increased use of cash rather than mobile money led to increases in robbery (Moore, 2020). In addition, according to aid workers and researchers interviewed, trade could not take place because taking produce to markets depends on a whole communication chain. Marketing the sesame harvest in eastern Sudan was severely affected, because without information about prices, farmers and agents were hesitant to market goods and no auction took place, affecting the livelihoods of many more. In conflict-ridden Darfur, mobile phones are necessary to communicate security information, not only about imminent attacks but also whether it is safe for displaced people to travel from camp to farms to work. Many people also use mobile banking as a safer means to keep money than banks. According to one interviewee:

> Now if you cut the internet and phone networks, people are lost. It becomes as if you are cutting off their source of life (Aid worker in Sudan, March 2022).

In Somalia, an aid worker expressed a similar view: 'Mobile money is more important than anything. It is the lifeline for everyone'. The population is highly dependent on telecoms and internet and disruptions are caused by a number of different actors in the context of a protracted conflict. In the early 2000s the US shut down one of the only internet provider and telecoms company, Al-Barakaat, because of suspected terrorist links, severely affecting money transfers (BBC, 2001).[13] However, means around

[13] US sanctions on the company were lifted in 2020. https://www.horndiplomat.com/2020/02/13/us-lifts-sanctions-on-somali-remittance-company-al-barakat/

this were quicky found through other platforms. In addition to forbidding social media, Al-Shabaab also disrupts mobile networks during military operations or to force the payment of taxes. In contrast, along the Kenyan border, the Kenyan Defence Force has attacked mobile phone masts over the past 2-3 years claiming to undermine Al-Shabaab operations. Given the population's heavy dependence on mobile networks this has a serious effect on livelihoods – even if this was not the actual intention. In some areas along the Kenyan border, this means people have to walk to where they can access telephone networks.

In places like Ethiopia, Sudan and Somalia, mobile networks and internet are an efficient way of maintaining social networks, transferring (and saving) money and has become the backbone of trade and market operations. However, their dependence also increases the effect of shutdowns or disruption. In Tigray, the only mobile phone and internet provider is Ethiotel, controlled by government, meaning it can easily be shut down. In Sudan, there are more providers but most are closely linked to government. There are alternatives, but they are expensive and not widely accessible (Ali, 2021). In Somalia, specific providers dominate each region and it appears that internet and mobile phone shutdowns has become one dimension of the conflict. In these populations, cutting off communications networks becomes an act of commission that effectively attacks production, markets, freedom of movement, and more. All of this needs more in-depth research. While almost all interviewees felt there were many advantages to the widespread use of digital technologies for the functioning of food systems, security, and aid provision, it was also clear to them that it led to a much heightened vulnerability, in particular in contexts with limited network providers and strong government control. In cases of civil war, such as in Ethiopia and Sudan, this proved particularly true.

Yemen and Syria provide two contrasting situations. In Yemen, although a large proportion of the population is dependent on remittances, communication networks function poorly and unevenly after seven years of war (Al-Bashiri, 2021)[14] and mobile money has not been authorised in areas controlled by the Houthi (officially called Ansar Allah, an Islamist movement that controls the north) (CALP, 2021b), possibly for fears of surveillance and loss of control. Most money transfers are done using a traditional *hawala* system, dependent on informal money transfer agents (although some have agreements with banks). This may also mean that network disruptions have less effect. The recent coalition attack in January 2022 on the only internet cable servicing Yemen, only lasted 96 hours but highlights the vulnerability of the country to internet shutdowns (Reuters, 2022). In Syria, networks also vary across the country depending on who is in control. In government areas, they are subject to disruptions and under close surveillance and infrastructure in some areas is poor. Tech-savvy users may be able to connect to other providers if one is shut down. Like in Yemen, digital aid is limited for these reasons[15] but also because of suspicion and the need for control (on the part of government), and the concerns around data protection (international organisations). A couple of interviewees argued that sanctions had a much bigger impact on the ability to transfer money to and within Syria, and that more access to digital technology would assist people in accessing food and money. The imanacard app is one example of technology enabling money transfers into unbanked crisis zones (https://www.amanacard.com/). **Based on these very preliminary findings, examining the dependence on mobile phone networks, the range of providers and state control or influence, can be an important consideration in determining famine risk through the effect of shutdowns.** However, if people are less dependent on digital technologies this does not mean they are not at risk of famine or humanitarian crisis. In some cases, they are in effect already cut off. As suggested before, examining risk of starvation or famine needs a holistic analysis with network connectivity and shutdowns being one factor.

[14] Information on the state of Yemen's telecoms network is conflicting. A CALP study reports network coverage and mobile phone ownership to be good ((CALP, 2021a).

[15] In the north-west which is outside of government control, NGOs have been providing cash transfers which have been digitalised to a limited extent. WFP is planning to pilot these too, given concerns over access with new border controls.

3.2 IHL and internet and phone network shutdowns

The previous section has shown that there are a number of cyberoperations in countries or food insecure populations, which may link to famine or where starvation may be used as a method of warfare. To summarise, these include:

1. Cyber disinformation campaigns (e.g., where civilians are fed a false narrative, experience social media bans, or targeted disruptions of particular accounts)
2. The deliberate disruption or shutting down of networks to enforce a digital and communications blackout (e.g., a state which shuts off its state provided internet or has the ability to coerce providers to do so).
3. Kinetic attacks on critical digital infrastructure, for example mobile phone masts and internet cables (or on the companies operating them).
4. Cyberattacks on critical infrastructure (the main references in the section above have been to humanitarian aid operations (rather than e.g., national food logistics systems or irrigation works).

While there is no specific mention of cyberattacks in the Geneva conventions or the Rome Statute, IHL is routinely applied to new developments and methods of warfare and cyber-warfare in our view is no exception. According to ICRC "there is no question IHL applies to, and therefore limits, cyber operations during armed conflict […]" (ICRC, 2019: 4). In other words, it can render useless objects that are indispensable to the survival of the civilian population, such as foodstuffs, crops, livestock, agricultural assets, and humanitarian personnel and consignments used for humanitarian relief operation.

The fundamental principle of IHL distinguishes between civilian and military objects, which is critical for the purposes of this report to determine the relevant status of the object in question (military, civilian, or as explained below an OIS – which is governed by a different protection regime). **Military objects** are those 'by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage'; **civilian objects** are everything else. The distinction of objects is part of the customary law and rules (described above) and applies in both types of armed conflict. (Sandoz et al. (1987), Henderson, 2009, Dinstein, 2016, Sassolli, 2017, Sassòli, 2019: 352-353.) Where an object serves both military and civilian functions, it may qualify as a military objective and could be legally targeted, its categorisation will ultimately be defined by its use.

OIS are considered in IHL as specially protected objects which benefit from a particular protection regime, in two respects (i) by prohibiting the attack, destruction, removal or rendering useless of such objects; (ii) even if these OIS could become valid military objectives, they lose protection from direct attack <u>only </u>if used exclusively as substance for the opposing armed forces or in direct support of military action. **It is always prohibited to take any action against OIS if it is expected to result in the starvation of the civilian population or to force its movement** (Sassolli, 2017)*:* 374-375). The term 'rendering useless' as found in the IHL and ICL definitions of the prohibition of starvation, has been interpreted to include a flexible range of operations, not limited to kinetic attacks or destruction (Gisel et al., 2020) and thus including cyber operations. Of critical importance in this context is the dual-use nature of communication networks for civilian and military purposes. Most cyber infrastructures will have enmeshed civilian and military networks, making it complex to assess what is or is not a legitimate military objective. It will depend on a holistic analysis of the specific network location of the attack and the other IHL rules of proportionality, precautions and the prohibition on indiscriminate attacks.

The Tallinn Manual on the International Law Applicable to Cyber Warfare explores the application of international law to cyber warfare and cyber operations. In the drafting of the Tallinn manual there was 'significant consensus among experts that IHL applies in cyberspace and that its basic rules and principles can and must be applied when conducting cyber operations during armed conflict' (Gisel et al., 2020). The Tallinn Manual prohibits starvation of civilians as a method of cyber warfare, although this prohibition is defined narrowly as "depriving a civilian population of nourishment (including water) with a view to weakening or killing it" (Rule 107 - Tallinn Manual).[16] It references the protection of civilian objects and OIS under Rule 141 of the Tallinn Manual and concludes with some reserved language of the permissibility of incidental starvation. It takes a cautious position.

The Tallinn Manual also identifies the relevant framework for humanitarian operations, and suggests that cyber operations which are designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance are also prohibited (Tallinn Manual Rule 145). Thus, the shutting down of a country's internet where it is infrastructurally indispensable to delivering relief may be assessed as an undue interreference with obligation to respect and protect such humanitarian operations.   The ICRC go further and suggest that these obligations in an international armed conflict can also protect the relevant data needed for the delivery of its humanitarian functions which are essential for the survival, health and well-being of the civilian population (Gisel et al, 2020: 329). This is further discussed in section 5.

Whether specific communications networks or their associated infrastructure would be held in any criminal trial to be an OIS would need to be assessed on a case-by-case basis, consistent with the continuous duty to assess the nature of a proposed target (principles of proportionality and precaution) and the case-specific nature of OIS particular to different climates, conflicts and civilian needs. Yet, it does not feel too far removed to imagine an investigation into individuals for the foreseeable harm, in terms of severe food insecurity, caused to a civilian population, by completely shutting down and rendering useless their communication networks over a sustained period of time.

4. Monitoring food security, famine and starvation crimes

As digital technologies have proliferated, humanitarian and human rights organisations use them to assess, monitor, and determine food security and famine risk and the effects of war on civilian populations. In recent years, the Integrated Phase Classification (IPC) for food security severity has become generally acknowledged amongst international organisations as the way that severity of food security is determined and famine is identified. According to the IPC, famine occurs when certain thresholds of food insecurity, malnutrition and mortality are crossed for a percentage of the population (Maxwell and Hailey, 2021).

Determining famine causation and starvation crimes is more complex. To understand famine, it is necessary to understand historical processes of marginalisation, and how political and economic processes interact to restrict access to food for some groups and to benefit others, as well as how specific acts lead to starvation. Determining whether an individual intended to attack, destroy, remove or render useless OIS with the specific purpose of starving a civilian population, needs an array of assessments. Evidence is needed on the nature, manner, timing and duration of any deprivations of OIS or attacks on civilians, including whether such attacks were long-term, persistent and/or indiscriminate; whether the attacks were widespread and perpetrated in an organised manner; and whether they took place as part of a campaign that systematically targeted civilians on account of their membership in a particular group (Jordash et al 2019, GRC and Mwatana for Human Rights, 2021).

[16] The rule based on Article 54(1) of the Additional Protocol I and Article 14 of Additional Protocol II, reflects customary international law in both international and non-international conflicts, citing to a host of military manuals.

This section focuses on the use of digital technologies in the assessment and monitoring of information on food security in hard to access populations (and where networks have not been shut down completely), what they can offer and for whom, and what some of the risks are. Technologies examined include: field-based monitors using apps (e.g. KoBo) on tablets or smartphones to collect and transfer data, mobile phone surveys and monitoring (sometimes using call centres), the use of satellite imagery, crowdsourcing (including streetmap), GPS tracking, and artificial intelligence (AI).

4.1 Role of digital technologies to food insecurity and famine

Constraints on access are often a major reason for not having enough data to determine the severity of food insecurity or famine. This may be because of insecurity (real or imagined) or government or warring party denial. Analysis and authorisation for publication may also take a long time, or never materialise in the case of the latter (Maxwell and Hailey, 2021). In theory, **digital technologies can provide one means of collecting information remotely when populations are hard to access, and provide a fast way of getting some basic information quickly.** Quantitative indicators of food security are a key part of the IPC (IPC Global Partners, 2021). These are indicators of food consumption such as the Food Consumption Score (FCS), Household Hunger Score (HHS) and the Coping Strategies Index (CSI).[17] Each rely on being able to collect simple recall data on foods consumed, experience of problems accessing food, and strategies used to cope. Together with information on the prevalence of malnutrition and mortality, and sometimes on livelihoods, shocks and vulnerabilities, a particular phase of severity is determined. Other famine early warning systems may collect regular information on market prices (e.g. Fewsnet).

The advantage of quantitative food security data is that they can be used to compare populations, and they are more easily collected remotely than qualitative information. The past decade has seen a dramatic shift in the way that humanitarian organisations collect data and in the kinds of data collected (Hagmann et al., 2021). In crisis situations, information collection has often changed from aid organisation staff interviewing face-to-face using paper checklists and notebooks, to subcontracting enumerators to enter data into tablets or phones, to contracting call centres to ask questions by phone. According to some of our interviewees, this has the advantage of speed as well as enabling access as no separate time is spent on data entry. In addition, some data cleaning happens immediately on entry, and GPS locators and voice recognition software can be used as cross-checks. An earlier study by two of the authors, in Somalia, found similarly that practitioners found tablets and a simple questionnaire useful to analyse food security quickly as data go straight from the field to Nairobi for analysis (Jaspars et al., 2020). Malnutrition and mortality data cannot be collected from a distance, although if field teams can measure weight and height, they can similarly enter the data on tablets and transfer it immediately for checking and analysis.

WFP, and other organisations, use these digital technologies for food security monitoring and vulnerability assessments. A variety of data collection apps exists.[18] The use of call centres to collect data by phone is now also commonplace and presents a particularly distanced way of interviewing (sometimes an organisation called geopoll.com is used). WFP uses this method worldwide for their mobile Vulnerability Assessment Mapping (mVAM) and to produce their hunger map (WFP, 2022b). Either completely randomly selected phone numbers or randomly selected aid beneficiaries are called, and data on food

[17] The FCS is a composite score based on self-reported information on nine consumed food groups and food frequency (number of days food groups were consumed during the past seven days), weighted by the ascribed relative nutritional importance of different food groups. HHS assesses whether households have experienced problems of food access in the preceding 30 days, as reported by the households themselves. CSI an experience-based indicator collecting information on household use and the frequency of five different food-based coping strategies over the past 7 days (IPC Global Partners, 2021: 38).

[18] Hagmann et al mention KoBo, Open Data Kit (ODK) Collect, Survey CTO, the ONA platform, but KoBo was mentioned more often by others, including in reports.

security is collected using voice calls, SMS, or chatbots. According to WFP, mVAM enabled rapid real time food security assessments in otherwise hard to reach areas in Yemen's emergency (WFP, 2016a). In Tigray, geopoll was able to conduct a phone survey in December 2020 but has not posted one since. While the data from Tigray was useful in providing information on displacement and market closures, the numbers reached were limited (46) (Elliott, 2020). At the same time in a face-to-face survey in Tigray in late 2021, WFP was not able to access western and southern parts (WFP, 2022a).

While remote assessments have some advantages for assessing hard-to-reach populations, there are a number of drawbacks and risks to assessing food security remotely. **First, the possibility of exclusions and bias.** Obviously, people without mobile phones will be excluded if assessments are done by phone (likely to be an issue in rural parts of Yemen) and others will not feel comfortable talking to outsiders by phone. In Sudan, for example, a long history of surveillance by the security services means it is extremely rare for anyone to answer the phone to an unknown number. Similarly in Al Shabaab-controlled or influenced areas in Somalia it may be difficult for people to speak freely by phone (although this is possible when relationships of trust have been established, see below). In some countries women are less likely to answer the phone than men (Hernandez and Roberts, 2018). Pilots in a number of countries reported low response rates, urban bias, a younger age and higher wealth group bias, misreporting of locations, and the need to speak the local dialect, although these are highly variable across settings (Mock et al., 2016). They also found food insecurity using this method to be consistently higher than in face-to-face assessments (ibid.).[19] **Second, remote technologies usually focus on simple quantitative information**, which is difficult to put into context without an on-the-ground presence or previous knowledge. As the WFP report on Tigray states: '...household-level quantitative surveys [are]… not suited to provide in-depth explanations of complex issues. Thus, questions on 'how' or 'why' are best suited to be explored through qualitative research methods' (WFP 2022a: 12). Qualitative methods need proximity, or an on-the ground presence, and if done remotely need in-depth contextual knowledge and a relationship of trust with those being interviewed. This has implications for analysing causality, in particular understanding the structural causes of food insecurity (and malnutrition), how the crisis is presented, and for humanitarian response (see below).

Artificial Intelligence (AI) is used in a range of humanitarian settings and for a number of purposes, but mostly for mapping and predictive analysis (Spencer 2021). Predictive analytics looks at patterns in past data and creates algorithms on the basis of statistical correlations. However, this depends on large datasets being available, and of good quality, which is rarely the case in famine-prone countries or populations. Attempts have been made at predicting famine using AI. Famine early warning analytics so far has only been piloted for drought situations (Lentz et al., 2021). AI could also be used to determine who is eligible for assistance but concerns have been raised about the possibility of poor data and algorithmic amplification, re-enforcing existing discrimination and inequalities (Spencer, 2021). Statistical correlations are not the same as causal relationships, which are impossible to determine statistically. More importantly, **the problem with famine prevention is often not an inability to predict famine or determine who needs aid, or having this information fast enough, but of the political choices** of donor and national governments and the actions of warring parties (ibid.). In the US and parts of Europe, such algorithms are already used to determine the eligibility of benefits claimants or the extent of surveillance they require (ibid.).

The invisibility of politics in digitalised food security assessments and famine early warning, is arguably the most concerning aspect of digitalisation. Contemporary assessments rarely consider the structural causes of food insecurity or how particular acts or power relations lead to famine. The IPC, uses its

[19] The article does not explain this finding, but does note that the difference between face-to-face and cellphone estimates is larger in situations of more severe food insecurity. It therefore suggests that cellphone surveys may be more appropriate in situations of chronic food insecurity (but also that they may be needed specifically in situations of severe conflict

own adaptation of a framework developed to examine the causes of malnutrition or mortality,[20] but structural or basic causes are vague (acute events, livelihoods assets, policies institutions and processes, and gender) (IPC Global Partners, 2021: 10), and pathways to food insecurity, malnutrition and mortality rarely explored in practice as part of the IPC analysis (and thus famine classification is not linked with accountability). In particular, it does not incorporate the political structures of power relations that influence food security (e.g. around trade, land ownership and access, labour relations, legal systems). AI also changes how we view the world, because it produces categories through which we think about ourselves and others (McQuillan 2018). Furthermore, digitalised assessments not only make politics invisible by removing political causes, but may also make the politically vulnerable invisible by excluding them (Jaspars and Sathyamala, 2021).

There are a number of possible explanations as to why structural or population-level social and political causes are rarely included in food security assessments. First, nutritionists and food security specialists (and other aid workers) consider these causes beyond their control. Second, examining structural causes turns food security assessments into a political exercise with possible repercussions for the people and organisations involved (Jaspars, 2019). This has become an issue particularly with the IPC, as it is usually government-led. With famine being associated with a failure of governance, governments – particularly those at war – use a range of tactics to stop famine being declared. Tactics range from preventing the collection of mortality data, denials of access, to tampering with data and preventing publication of assessments (Maxwell and Hailey, 2021). Government officers involved may be fired and international organisations expelled. Presenting an apolitical picture of food insecurity (with unobjectionable quantitative outcome data) therefore also has functions in that it enables organisations to remain present, continue their operations and maintain their budgets. It also means, however, that the causes of famine or starvation crimes remain hidden (Jaspars, 2018 and 2019, Jaspars et al., 2020).

With famine being associated with a failure of governance, governments – particularly those at war – use a range of tactics to stop famine being declared.

4.2 Gathering evidence of starvation crimes and engaging with armed actors

When considering IHL violations and famine risk, questions of how and why (and who) are important, which cannot be answered by quantitative data on food security alone. Quantitative measures of food insecurity say little about its nature, its underlying causes or the risks associated with strategies adopted in the midst of war (Jaspars, 2018: 56). Determining starvation crimes, in contrast, is about putting the politics back into analysis of famine. This section considers what evidence digital technologies can provide to help determine starvation crimes.

Famine researchers and experts in international law have recently started analysing how attacks on OIS may contribute to hunger, how to investigate these violations, and how to hold actors responsible ((Hutter, 2015, De Waal, 2018, Jordash et al., 2019, GRC and Mwatana for Human Rights, 2021, Dannenbaum, 2021, Conley et al., 2022). In the growing body of literature on starvation crimes, a common theme is the neglect of this subject matter, the lack of investigations, and the dearth of prosecutions. One question addressed by researchers is to understand the reasons behind this neglect, to provide a roadmap for future prosecutions (Jordash et al., 2019), and a forum to air the highly divisive instances in which states deliberately starve their own citizens (Hutter, 2015; De Waal, 2018). A recent analysis of starvation in Yemen contains novel rigorous investigative reporting and forensic legal analysis to draw legal conclusions on

[20] An adaptation of the UNICEF framework on causes of malnutrition (UNICEF, 1990).

responsibility (GRC and Mwatana for Human Rights, 2021). Researchers and legal analysts also explore outside of criminal accountability what other avenues for transitional or restorative justice may be viable and indeed preferred (Conley et al., 2022).

Digital forensics and remote interviews with human rights organisations or monitors and investigators on the ground have played a key role in putting together evidence for starvation crimes in Yemen and Tigray. Remote technologies used by Global Rights Compliance and their partners include: Satellite imagery, Open-Source Intelligence (OSINT) on food price fluctuation; NASA's Fire Information for Resource Management System (FIRMS) to identify increases in fire points which may indicate scorched earth tactics; Social-media Intelligence (SOCMINT) to uncover telegram and YouTube channels containing visual, audio or documentary footage. Satellite imagery can be used to monitor the destruction of houses, farms, markets, monitor market activity, populations movements. It has been used to help provide additional information in building a case on starvation, with imagery of scorched earth tactics, for example in Tigray (WPF 2021) or Darfur (Radio Dabanga 2020); or aerial bombardment campaigns in Yemen to identify whether agricultural areas have been deliberately targeted and destroyed and food producing facilities functional (GRC and Mwatana for Human Rights 2021). Satellite images have also been used to map displacement or estimate the number of people affected, for example in Myanmar (see for example: Human Rights Council, 2018). More closely related to food security, satellite monitoring of market activity in Tigray has recently been set up (Von Carnapp, 2022). Open street map (GIS), and crisis mapping using social media, are other examples (Twitter, SMS) (Thomas and Obrecht, 2016). 'Ushahidi' used these tools in the Haiti earthquake and later in Libya to map information on public health, security concerns and infrastructure damage. In Libya, however, concerns around quality control, privacy/confidentiality, and safety concerns were noted (Burns, 2014).

Digital or remote evidence has no doubt enhanced the capability of those investigating IHL violations, ICL crimes and human rights abuses. However, while it adds to evidence on starvation crimes, like with the quantitative remote assessments discussed above, there are risks of bias, exclusion, and causal links still need to be established. The war in Ukraine, for example, has highlighted the issue of 'deep fakes' and 'planted evidence' and it may be difficult to determine the competence and objectivity of online reports by citizens, journalists and investigators. The ethics of gathering intelligence from social media also needs to be considered further (Privacy International, 2017). Determining causality and intent of IHL violations, requires establishing the perpetrators' awareness of, and proximity to, relevant deprivations. To assess whether armed actors have a specific purpose to starve civilians, and the requisite intent under ICL, at a minimum, four factors should be considered. Did the armed actors:

1. Have an awareness of the risk that interference with OIS would lead to starvation (including where the deprivation occurs in pursuit of an ostensibly lawful purpose);
2. Show respect for the full range of relevant IHL prohibitions (including the prohibitions on indiscriminate and disproportionate attacks; the prohibition against terrorising the civilian population; the prohibition against collective punishment; the prohibition on the use of human shields and the prohibition against displacement);
3. Implement any of the positive obligations flowing from IHL principles applicable in the context of the conduct of hostilities; and
4. Implement any concrete steps to alleviate civilian suffering, especially those that are capable of facilitating delivery of OIS to affected civilian populations.

Digital technologies add to the information available to answer these questions, and provide a key resource for hard-to-access populations. As mentioned above, however, in assessing starvation crimes in

Yemen and Tigray, remote digital information was combined with phone interviews and in-depth qualitative information gathered by human rights investigators and monitors on the ground. Remote qualitative information gathering is possible when analysts have in-depth contextual knowledge and a relationship of trust with analysts on the ground. It should, however, not replace on-the-ground information collection and analysis when possible.

In contrast to an IHL violation, establishing the war crime of starvation does not require as a matter of law, demonstration of a causal link between an attack on OIS and resulting starvation, suffering or death of civilians arising from the attack. Death or suffering is not one of the Elements of Crime of the war crime of starvation under the Rome Statute. Establishing causation is important as a matter of evidence, not law. This is not to argue that the consequences of any deprivation will be irrelevant to an assessment of individual criminal responsibility, the intent of starvation remains a significant factor when assessing the likelihood of famine.

Once evidence is obtained on potential starvation crimes, it can be used outside of criminal proceedings in the ways described below. From our interviews, and because of the political repercussions noted above, NGO or UN programme or logistics staff who gather information on food security, rarely engage with armed actors directly. Since 2018, however, FAO and WFP report to the UN Security Council on Resolution 2417. OCHA writes closed White Papers for the attention of the security council, and individual donors (like FCDO or the EU) are able to do this too. Otherwise, information can be channelled in the following ways to hold warring parties to account include:

1. UN procedures to submit complaints against states on behalf of victims, to highlight gross patterns of human rights violations and advocate for legal and policy changes. Including: the Human Rights Council Complaint Procedure and treaty-based bodies such as the Special Procedures of the Human Rights Council, and the Monitoring and Reporting Mechanism established by the UN Security Council to address children affected by armed conflict (CAAC), and the various human rights treaty monitoring bodies. Other mechanisms include: country- or conflict-specific fact-finding missions, commissions of inquiry, investigative mechanisms and expert groups established by the UN General Assembly, the UN Security Council, or the UN Human Rights Council.
2. Engaging with the UNSC pursuant to UNSC 2417. The UN Secretary-General has to provide information on the risk of famine and food insecurity in countries with armed conflict as part of his regular country-specific reporting, and also to report swiftly when the risk of conflict-induced famine and wide-spread food insecurity in armed conflict contexts occurs. Reporting on the implementation of UNSC 2417 is scheduled annually, with strong calls for increased and transparent reporting. (Open Debate at the UNSC on Conflict and Hunger, 19 May 2022[21])
3. Sanctions to address starvation crimes. This is an option specifically identified in UNSC 2417 (See Spatz et al., 2022 for more information). The UN, the EU, various Northern American and individual European states have sought to use sanctions targeted at individuals and entities deemed responsible for human rights violations and/or international crimes, under which they have also occasionally considered starvation-related conduct (GRC, 2021, GRC, 2022).

[21] https://media.un.org/en/asset/k10/k10mjpv1u3

Examples of local actions are rare, although we did find an example, in Sudan, following the internet shutdown in June 2019, where a lawyer first brought a case against his cellphone provider for breaking his contract (which ensured access to the internet) and later a class action to restore internet services to other customers (Moore, 2020). According to Moore:

> It's hard to overstate the incongruity — the absurdity, even — of arguing the finer points of contract law in the wake of a civilian massacre, before a judge who answers to an unaccountable military regime. And yet, there's nowhere but local courts to turn to when the government takes away the internet. There's no international treaty protecting internet access, no global legal body that sanctions a rogue government or cellular provider.

Some resistance came from within the telecoms companies as well – engineers switched some people back on so they could communicate with the outside world. Local actions in Sudan also raise another issue – that analysis using digital and remote technologies does not include local participation, and local participation – and resistance – is crucial in preventing famine.

In conclusion, digital technologies have provided a means of accessing conflict-affected populations who cannot be reached physically, and who are potentially at risk of famine and starvation. They can provide some information on food insecurity and famine risk and provide a source of evidence for starvation crimes, but a number of limitations need to be taken into account. There are potential issues of bias, exclusion, interpretation. The necessity for the speed with which digital data can be gathered needs to be questioned. Understanding causation, however, and the complex dynamics of famine, requires more in-depth qualitative information gathering which can be done by phone if interviewers have existing knowledge and relationships of trust (if network connections are functioning of course). When using remote digital technologies to gather mainly quantitative information, it is important to consider what has been lost (compared to being on-the-ground). In addition to removing politics and limiting causal reasoning (also see Duffield, 2018) the removal of human interaction between aid worker or researcher and crisis-affected people, also reduces empathy (and thus the humanitarian imperative) which makes it easier to reduce material assistance and in turn re-enforces the drive towards digital aid (Jaspars, 2018). These issues are discussed further below.

5. Digital humanitarian aid, access, risks and principles

The last decade has seen a trend towards the digitalisation of humanitarian and food assistance, stimulated by the 2008 food and financial crisis, and later the Covid-19 pandemic. The current global food crisis is likely to accelerate this trend further. In situations of conflict, a key area to examine is whether and how digital technologies may enable access, not only for assessments but also for aid delivery, and the ways in which they can be blocked. The authorities controlling a particular area must provide civilians with the means of survival, and if they cannot or will not – they are obliged to allow access for impartial humanitarian organisations. In addition to the potential for blocking digital aid, concerns have been raised about new forms of exclusion, the sharing of sensitive personal data, and surveillance, putting already vulnerable populations at greater risk. Private sector involvement in digital technologies (telecoms companies and internet providers, banks, data management companies, search engines, social media platforms) raises issues of neutrality, impartiality and independence in humanitarian action. While some of these risks are not strictly violations of IHL, they have implications for the protection of civilians and are likely to disproportionately affect populations already vulnerable to famine. This section starts with a brief overview of the digitalisation of aid, followed by a discussion on access, risks, and humanitarian principles.[22]

[22] Unfortunately, space and time did not allow us to examine digital fundraising campaigns for famine relief, whether by organisations or citizens

5.1 The digitalisation of humanitarian aid

Digital technologies used in aid delivery include biometrics (iris scans and fingerprints) for registration and identification, debit cards, banking services, mobile phone cash transfers, digital platforms (for various food and agricultural services) and algorithms to predict need. The focus in this section is on the first three as being the most common at the time of writing. Cash transfers are increasingly part of humanitarian action, especially following the World Humanitarian Summit in 2016, where the increase was agreed as part of the Grand Bargain between donors and humanitarian organisations. The advantages of cash as aid have long been reported as providing choice, maintaining the dignity of crisis-affected populations, efficiency and accountability (Harvey, 2007). The use of biometrics and other aspects of digital identities are promoted largely in order to prevent fraud (The Engine Room and Oxfam, 2018, Holloway et al., 2021). Cash transfers have also been promoted as ways of delivering aid remotely in situations of conflict to overcome access restrictions (Sandvik et al., 2014), and this trend has massively accelerated during the Covid-19 pandemic when people were ordered to stay at home or socially distance (Bryant et al., 2020, CALP, 2020, Hamilton, 2021).

WFP is a key actor in the digitalisation of humanitarian assistance, in particular food and cash assistance. Its digitalised assessment methods were discussed in section 4.1. In addition, it has developed SCOPE, a biometric beneficiary identification and benefit management system (WFP, 2016b). WFP promotes its SCOPE system because it can store a range of demographic and food security data as well as biometrics, and can be linked to a range of interventions (including from other actors). They argue it removes the possibility of duplicate registrations, thus reducing fraud and corruption. WFP uses a wide range of additional digital technologies for: partnership agreements, logistics, financial systems, staff management, as well as assessments/decision-making and ‘knowing beneficiaries better’ (see page 5 in (WFP, 2022c). SCOPE and the programme side of cash transfers (e.g. targeting) falls under the latter and we focus on this as it is concerned with aid delivery. A number of other humanitarian organisations also use debit cards, or bank cards and banking services, mobile money transfers as part of their operations.

5.2 Digital aid and access to conflict-affected populations

Instinctively it seems that digital cash transfers should provide greater access to conflict-affected populations. It does not need convoys of trucks that may need government authorisations to move, that get stopped at checkpoints, or attacked or diverted by armed groups or robbers. Mobile money can be sent direct to people in hard-to-reach areas, and bank cards can be used in places that people have been displaced to (providing there is food to buy). These are real advantages. In Ukraine, ICRC has been able to continue to provide cash transfers to people who were previously beneficiaries in the east of the country. Some beneficiaries of existing social protection programmes in Ukraine have also been able to receive their benefits in areas they have fled to, and these existing systems may be used for humanitarian assistance (Sojka et al., 2022).

However, a number of interviewees argued that for newly conflict-affected populations, registration of beneficiaries still needs an on-the-ground presence (even if only sporadic). Others argued that for populations completely cut off, it may be worth taking the risk of working directly with telecoms providers to transfer money without having detailed information on the beneficiaries. These issues were raised in particular for **areas held by listed groups, such as Al-Shabaab in Somalia and Boko Haram in Nigeria**. Such situations raise a number of ethical issues about the risks associated with digital technologies. In addition to any potential taxation by designated terrorist groups, there are questions about the risk associated with identifying and mapping people in these areas as part of cash transfers. How does this compare with the risk those same people would face if displaced and living in camps in government areas? Related questions are who makes those decisions and whether aid workers have sufficient knowledge about digital aid to explain, to beneficiaries what happens to the data collected – and generated - as part of mobile cash transfers (these issues are explored in more detail in the following section), and be accountable. In Yemen, the Houthi refused for WFP to gather biometric information in areas under its control, because they considered it a challenge to their sovereignty (Weitzberg et al., 2021). Furthermore, they accused WFP of being political and of gathering intelligence, which was given credence by the controversy over WFP's partnership with Palantir, a US algorithm intelligence firm also connected to the CIA (Clausen, 2021).

According to our interviewees, **the bigger issue is government aid blockades or access denials**. As we have seen in section 3.1 if a government wants to block aid going to a particular area or population group it can do so whether aid is digital or material. Network shutdowns have this effect, even if originally activated to limit the enemy actions or to prevent information on crisis coming out. Monitoring of blockages of food convoys by non-state armed groups did not appear a big issue from our interviews. Suggestions that digital technologies, e.g. GPS or mobile phone tracking may assist with access negotiations, resulted in responses that food (and other aid) transport is usually done by the private contractors and it is they who negotiate to get food to where they are contracted to take it to.

A couple of broader issues need to be mentioned under access. One is the danger that **remote, digital cash transfers – and limited access - become the default options in conflict situations.** Cash transfers become the multi-purpose solution but cannot address protection risks. It may even create some (see below). Aid organisations may be tempted to continue to work remotely when it could be possible to start work on the ground, or warring parties (including governments) deny physical access on the basis that aid can be provided remotely. While usually planned as a short-term measure, remote management often ends up being a long-term arrangement. When aid workers spend time outside of the conflict area, they lose their familiarity with the situation on the ground, their working relationship with national staff changes and they become more reluctant to return (Stoddard et al., 2010). Sudan and Somalia provide good examples of what happens when information on nutrition and food security is mainly quantitative and assistance provided digitally and remotely. Such aid practices create an image of technical progress (new quantitative food security indicators, new modalities of cash transfers, which can be administered remotely) in which conflict and the manipulation of aid came to be hidden as the cause of food insecurity (for more on this argument see Jaspars 2018; Jaspars et al. 2020).

Finally, digital technologies add a **new dimension of access: access to data** and who has it. With the production, storage, and processing of increasing amounts of sensitive digitalised data of humanitarian beneficiaries comes the question of how to ensure they know what happens to their data and consent to the ways in which it is used. Arrangements are needed to prevent access by (nefarious) actors whose uses may undermine rather than buttress the security of these digitalised humanitarian subjects (Jacobsen and Fast, 2019). This is discussed further below.

5.3 "Doing no digital harm" – risks for populations already vulnerable to famine

Like for all humanitarian response, digital assistance entails risks as well as benefits. A number of recent publications refer to "doing no digital harm" (Cohen, 2018, Privacy International and ICRC, 2018, Mebur and Kwamy, 2019, Burton, 2020). Doing no harm, protection and conflict sensitivity have become key aspects of humanitarian action over the past two decades, and can refer to attempting to minimise any potential negative effects of aid: risks to beneficiary safety, reinforcing unequal power relations, bias or inequalities, undermining local capacities and more. Issues that come up regularly in relation to digital technologies, are the potential for new types of exclusion, data protection (and privacy) and surveillance for political and economic purposes. The expansion of cash transfers gives aid agencies and donors access to vast amounts of data about the identities and habits of cash beneficiaries, leading to a situation of simultaneous care and harm (Jacobsen and Fast 2019). In reality, as all aid programmes will have effects beyond their stated objectives, the issue is to understand the wider economic and political effects and mitigate any potential harm for vulnerable civilians. In humanitarian law, these are issues related to **the protection of civilians**. **The risks associated with digital technologies relate to famine because it is the most marginalised and famine prone populations that will be most affected. Any famine prevention efforts must therefore be able to analyse and address these issues.**

Digital cash transfers entail both **old and new forms of exclusion**. The risk of under-registration or exclusion of politically marginalised groups, or the taxation of the assistance they receive, issues familiar to humanitarians working in conflict, remain the same. New forms of exclusion include those due to limited connectivity (or electricity to charge phones), no mobile phone or not being familiar with its functions (limited digital skills), or that those without ID cards are unable to open bank accounts or set up mobile phone contracts (Bryant et al. 2020). Depending on context, women, migrants or refugees, or particular ethnic groups may not have national ID cards, thus potentially exacerbating existing discrimination and inequalities. Technical failure, in terms of reading iris scans and finger prints has been another reason (Holloway et al. 2021). Forms of exclusion may be created if money can only be retrieved through finger print of iris scans at particular outlets thus requiring beneficiary mobility. In Somalia, recent research also found a new form of exploitation with mobile cash, in that it was easier for employers not to pay casual labourers if they were not familiar enough with the technology to check and complain (Chonka and Bakonyi, 2021).

> With such centralised digital data, particularly in situations of conflict, it is necessary to ask how the technology can be weaponised, and how new authorities will be using the digital identities created earlier.

Arguably a bigger issue, from the perspective of rights, famine risk, and starvation, is who **has access to the digital beneficiary data, and whether civilian data are objects to be protected under IHL.** Interviewees working on digital risk pointed out that centrally held information on digital identities can be politically controlled, and lead to politically motivated exclusions or even persecution. Benefits, bank cards, or humanitarian assistance, to certain population groups could simply be turned off (and which happened in Tigray). With such centralised digital data, particularly in situations of conflict, it is necessary to ask how the technology can be weaponised, and how new authorities will be using the digital identities created earlier. Recent examples of digital data falling into the wrong hands are those collected by UNHCR on Rohingya refugees shared with the Myanmar government and by humanitarian and military organisations in Afghanistan – and later accessible to the Taliban (Holloway and Lough, 2021, Jacobsen and Steinacker, 2021). In contexts where governments have a history of marginalising certain sections of the population, as with the Rohingya, this risk is increased. Opinion currently varies as to whether (digital) data are protected under IHL. However, 'if data are deleted or manipulated in a manner that is designed or expected to cause, directly or indirectly, death or injury to a person, … the operation is an attack regardless of whether data themselves constitute objects for the purpose of IHL (Gisel et al., 2020: 317). Furthermore, the same authors have argued that with the modern meaning of objects in today's society, interpretation of the term in light of its object and purpose, it can be concluded that "data is an 'object' for the purposes of the IHL rules on targeting" (quoted in Gisel et al, 2020: 318).

Humanitarian organisations have already started examining the risks (as well as the benefits) posed by their digital transformation. The UN Legal Digital Identity Task Force (set up to ensure a legal identity for all) recognises the potential for such identities to **replicate existing inequalities, discrimination,** and the need for caution in fragile and unstable situations (Arraiza, 2022). WFP recently conducted an evaluation of its use of technology in constrained environments (defined as environments where access is limited due to insecurity or physical obstacles or where there are barriers to the use of digital technologies due to poor networks coverage or political restrictions). This evaluation concluded that, while WFP's use of digital technologies had made significant progress in tailoring assistance to needs, issues that needed to be addressed included, data protection, the top-down nature of digital technologies, insufficient briefing of beneficiaries about what would be done with their data, and insufficient staff knowledge and training (WFP 2022c). Overall, the evaluators concluded that WFP needed strategic clarity on contentious issues such as the use of biometrics, public-private partnerships, and digital services to government (ibid). A recent audit of SCOPE found it to be only partially satisfactory in relation to governance arrangements and risk management (WFP, 2021).

Even organisations with data protection expertise are not immune to **cyber-attacks**, as shown by the recent attack on ICRC (2022) which highlights the vulnerability of humanitarian organisations as they digitalise. Cybersecurity is generally less developed in the global South (Schia, 2018). Furthermore, in authoritarian or unstable contexts, governments may require or force telecoms and other service providers to hand over personal information, or the necessary laws on data protection simply do not exist (for example in Somalia: see Hujale, 2020). Data minimisation is becoming a key principle of data protection; i.e. only collecting the data necessary for programmes implemented, rather than the frequent practice of gathering more information than is generally analysed. Another suggestion is that, particularly in political unstable contexts, not to rely completely on digital technologies and to have back-up plans. In Sudan, an interviewee noted the hacking of individual mobile phones as an issue; people may be sent false vouchers or bank statements to entice them to release information about their accounts. His particular concern was with IDPs receiving these kinds of messages from what appeared to be respectable financial institutions. As the use of digital technologies increases, so will the rise of ransomware and cybercrime, which is likely to affect already vulnerable people most.

The scope for surveillance is a significant harm associated with digital technologies. At its simplest, this can entail the monitoring of registered people's movements and expenditure. According to one interviewee, in Afghanistan people asked not to receive mobile money as it meant they could be geolocated, potentially putting them at risk. In Lebanon, according to another interviewee, Syrian refugees did not want to register for fear of their data being shared. Technologies, mobile money and bank cards for example, also create **metadata,** which create profiles based on who is transferring money for what purposes, when and where (Sandvik et al., 2014). If accessed by other parties, these profiles can be used for ad targeting, commercial exploitation, surveillance, discrimination and persecution. For example, the financial institution used by aid organisations can categorise the cash aid beneficiary as a potentially non-trustworthy borrower. The 'know your customer' regulations of banks mean they will gather as much information as possible (Privacy International and ICRC 2018), in contrast with necessary security regulations by humanitarians. Some of our interviewees argued, however, that surveillance may not be an issue where mobile money transfers as aid are minimal compared to cash transfers overall (in particular when using existing accounts for aid transfers), for example in parts of Somalia, or where surveillance is already extensive, as for example in Syria (but also others mentioned in this paper). Interviews in Syria and Yemen, revealed that mobile cash transfers as aid is extremely limited.

Finally, several interviewees pointed out that in some conflict situations cash transfers may not be appropriate in any case because of high rates of inflation (Sudan, Syria), or because food is not available in the markets (Tigray). General market assessments are still needed.

5.4 Humanitarian principles

Humanitarian principles provide a framework for providing assistance in situations of war, and to maintain access to all conflict-affected populations. The key principles are humanity, impartiality, neutrality and independence. As will be clear from the previous sections, digital technology has the potential to compromise all of these. First, the principle of humanity – the alleviation of suffering wherever it is found - entails a degree of empathy which lessens with distance (Slim, 2015). With digital technologies much of the human element is removed, replacing human connection with a digital interface and turning people, and their needs, safety and dignity, into data (Devidal, 2021). This can make it easier to withdraw assistance in protracted conflict situations, or from particular population groups, but does not reflect the complexity of their reality or the causes of food insecurity and famine.

The potential exclusion of vulnerable or marginalised groups, as discussed above, compromises the principle of impartiality, the relief of suffering solely on the basis of need. UN Human Rights rapporteurs have flagged the risk of racial discrimination through digital technologies ((Alston, 2019, Achiume, 2020). Discrimination and bias is amplified in the algorithms produced through artificial intelligence, as the data on which they are based are subject to human biases. The issue with decision-making based on algorithms, however, is that they are impossible to challenge (decisions are based on statistical correlations rather than reasoning). Digital technologies are not neutral (not taking sides in hostilities), as they may be aligned to the political (and economic) priorities of those who create and promote them, including tech companies (telecoms, internet, data management), banks and financial service providers and governments (Devidal, 2021). As we have seen above, they can provide the means for surveillance and oppression. Finally, independence requires organisations to maintain autonomy to be able to act in line with the principles. The extensive private sector involvement makes this difficult. Private companies are motivated by profit rather than humanitarian considerations, and profits can be made not only through providing the requested services, but perhaps also by selling additional financial services (insurance, credit, savings plans) or customer profiles and data. A wide range of companies are involved, from local turned global telecoms companies such as Hormud in Somalia, or global companies such as Microsoft, Google, Facebook or Mastercard. The former has become one of the most powerful actors in Somalia, investing in all elements of the food chain (aid, production, trade, import/export) (Jaspars, et al. 2020), and the latter are increasingly involved in humanitarian assistance which provides them with new markets (Spencer 2021).

Finally, although not strictly related to humanitarian principles, there are issues of local participation, choice and the localisation of humanitarian assistance. The latter was also a commitment in the Global Humanitarian Summit and the former are generally acknowledged as good practice if not principles of humanitarian assistance. The adoption of digital technologies, however, is pulling humanitarian assistance in the opposite direction, leading to accusations of techno-colonialism. Digital technologies are developed and decided on by private companies and – often – international organisations or governments, sometimes in partnership. Recipients are given little information on the use of their data, the risks, or a choice in how they receive assistance (even cash transfers can be cash in hand or vouchers rather than mobile money or smart cards). The use of algorithms is particularly contentious in this regard: ‘by claiming neutrality and universality, algorithms assert the superiority of abstract knowledge generated elsewhere. By embedding the logic of the powerful to determine what happens to people at the periphery, humanitarian AI becomes a neocolonial mechanism that acts in lieu of direct control’ (McQuillan, 2018).

5.5. Digital aid and IHL

Throughout section 5, a number of issues were raised about access, risks and protection, in relation to IHL. The first is that digital aid can be blocked by warring parties, just as material aid can be. IHL therefore applies in the same way, in that warring parties are obliged to provide for the rapid and unimpeded passage of impartial humanitarian aid. These rules are also reflected in The Tallinn Manual which identifies the relevant framework for humanitarian operations in the context of cyber warfare. Cyber operations which are designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance are also prohibited (Tallinn Manual Rule 145). Thus, the shutting down of a country's internet where the internet is infrastructurally indispensable to delivering relief (e.g., via the provision of cash transfers via mobile networks) may be assessed as an undue interreference with obligation to respect and protect such humanitarian operations.   In addition, as section 5.4 discusses there may be new issues to consider as to whether digital aid can be truly neutral, impartial and independent, given the extensive private sector involvement.

A new area is digital data and who has access. In section 5.3, we suggested that centralised data systems could potentially be abused by authoritarian or oppressive regimes to cut off welfare or for persecution. According to Gisel et al. (2020), it could be argued that data are a humanitarian object under IHL if their manipulation or deletion caused injury or death to a person.   This also relates to cyberattacks on humanitarian organisations holding these data, or on their computer systems generally (and thus disruption other operations such as cash transfers, health care, etc). OIS can include the infrastructure that is required for the functioning of the indispensable object (Tallinn Manual, Rule 141, ICRC, 2019), meaning that the digital technology required to facilitate humanitarian aid, could in principle be deemed an object indispensable in its own right.

As suggested in section 3.2, given an OIS will be likely interpreted in any future court proceedings in a context specific manner, whether or not a specific object will be deemed an OIS in a particular context and thus considered a specially protected object under IHL is not a material factor to determine in this report (for the avoidance of doubt, this assessment would be material in a hypothetical court case). Cyber crime on individuals appears to be an increasing risk and needs further exploration.[23]

6. Conclusion: issues to consider about digital technologies, IHL and famine risk

For many people, digital technologies have become absolutely essential in every aspect of life: food systems, livelihoods and survival – ranging from access to social networks, remittances, banking, trade and markets, as well as information on security and labour opportunities. In conflict-affected countries, and those vulnerable to food crisis and famine, humanitarian organisations have increased the use of digital technologies in assessments, monitoring and response, over the past two decades. For all of these, the use of mobile phone and internet technologies are common – for food security and famine assessments, for beneficiary identification, and for cash transfers for example. A key advantage of these technologies is thought to be the possibility of assessing and providing assistance remotely to conflict-affected and inaccessible populations. Remote quantitative assessment technologies are frequently used for food security assessments, to provide information on severity of food insecurity. Similarly, satellite imagery

[23] Analytically, it remains at this stage unsettled as to whether digital technologies involved in the provision of humanitarian aid would be deemed an OIS in their own right (as per the Tallin Manual and ICRC) or rather as critical civilian infrastructure required for the functioning of downstream indispensable objects such as the humanitarian aid (cash transfers and the like) or the indispensable functioning of health facilities or food and water services. Notwithstanding this legal observation, the centrality of digital technologies as infrastructure or otherwise, in humanitarian response is reinforced.

and a range of social media and open source intelligence information has become a key part of the investigations carried out by international legal experts to gather evidence of humanitarian law violations and starvation crimes.

At the same time, the penetration of technologies into people's lives has made some people and organisations more vulnerable to disinformation and to network shutdowns. Disinformation has long been a part of conflict (about the enemy or the causes of conflict), but social media has the potential to reach a larger audience more quickly, thus potentially increasing tensions (as was shown in South Sudan). In conflict, governments or other warring parties sometimes shut down networks (partially or completely) because they want to stop communication between enemy forces or between protestors, or to prevent information about the conflict and crisis reaching the outside world. Our interviews showed that it could also have the effect of stopping money transfers (including aid), agricultural sales, and trade. Preliminary findings suggest this depended in part on the number of providers and their links with government or the power of government or military officials to shut down communication networks. This needs further exploration.

Our analysis, indicates that shutdowns (as a cyberoperation) can deprive people of objects indispensable to their survival and therefore could be considered a violation of international law. While the dependence on technology and the vulnerability to cyberattacks can be an important factor in starvation risk for some, this does not mean that those with little dependence on mobile technologies are better off. Mobile technology does not function well (or freely) in Syria and Yemen, for example, but the populations face multiple other risks to their food security. They are in effect already 'shut down' – and may actually benefit from greater connectivity. These issues need further in-depth research. In food security and famine analysis, the main emphasis needs to remain on analysing historical marginalisation, political and economic processes and decisions that create risk of starvation and famine for particular groups. What this paper highlights is the importance of an additional step to analyse whether and how digital technologies influence food security, inequalities, conflict narratives, and war strategies.

As part of humanitarian assessments and response, and identifying starvation crimes, digital technologies have limitations and risks as well as advantages. Digital information provides additional evidence, but establishing causality (which is crucial in establishing whether IHL violations lead to starvation), remains difficult and in-depth qualitative enquiry remains important. Such enquiry can be done remotely, if researchers or assessors have contextual knowledge and trusted relationships with those on the ground. The danger of remote digital assessments becoming the norm also needs to be considered. For some organisations there may be a temptation to continue working remotely because it is cheaper and less risky. Warring parties may start denying access on the basis that assistance can be provided remotely. Over time, this can lead to distorted understandings of political processes and famine causation, and even hide much of the political dimension from famine. In contrast, a focus on starvation crimes has to mean putting the politics and political analysis back into an analysis of famine causation.

In terms of access to aid, the advantages of digital aid appear to be few,[24] mainly when programmes had been established and access lost because of the outbreak of war – meaning cash transfers could be made to previously registered populations. However, if a warring party (usually a government) wants to block aid, it can generally block digital as well as material aid. Some risks of digital aid in conflict remain the same: for example issues of under-registration of marginalised groups and taxation. There are also new exclusions: due to limited connectivity or mobile phone ownership, or the need for ID cards, which may further feed into existing inequalities and vulnerability to food insecurity and famine. Migrants and displaced populations, also amongst the most vulnerable to famine, are often worst affected by exclusions. The use of algorithms in early warning and beneficiary selection may further exacerbate these trends, as

[24] Advantages in terms of efficiency, market stimulus, dignity, choice remain

does the extensive involvement of private sector whose aim is profit rather than humanitarian concerns. That the private sector benefits from aid is of course not new, but the engagement of new actors and organisations needs careful analysis.

Issues of data protection and surveillance are new areas of exploration for IHL. If authoritarian or oppressive governments have access to centralised digital identities, they can use this to exclude or persecute particular population groups or political opposition. Some legal analysts argue that data, thus including beneficiary data, can be considered a civilian object under IHL and their manipulation considered an attack if it leads to injury or death. Government agencies, technology companies and aid organisations have all been subjected to cyberattacks, indicating the need for greater caution. It also highlights the need for back-up non-digital options in aid delivery. Finally, the neo-colonial nature of digital technologies needs serious attention in the field of famine prevention. If data is decided on, extracted, and used by outsiders from the Global North, it will undermine local anti-famine political action. Local political action is as important as international action in preventing famine.

This paper has raised many issues related to the use of digital technologies in food systems, livelihoods, and war, and in humanitarian and human rights assessment and response. The digital transformation of societies has important advantages (communication, information, money transfer, mobile banking) but in some conflict situations they have introduced new vulnerabilities. Each of these issues we highlight need further in-depth and on the ground research. In this, it is important to consider what really has been gained with the digital transformation, and what has been lost. With further evidence, it will also be important to further examine the legal dimension – when do digital networks or personal data constitute an OIS? How can the evidence be used to engage with armed actors? And by whom? With this paper we hope to have started a conversation on these issues, to have stimulated practitioners to take these issues into account in their programming, and to lay the groundwork for further research. This will be all the more important with the anticipated acceleration of digital technologies in responding to the current and worsening global food crisis.

REFERENCES

Achiume, E. T. (2020) *Racial discrimination and emerging digital technologies: a human rights analysis. Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance,* New York: UN Human Rights Council.

African Arguments (2022) 'Four ways the Ethiopian government manipulates the media', available at https://africanarguments.org/2022/02/four-ways-the-ethiopian-government-manipulates-the-media/, accessed 18 March 2022.

Ahmed, K. (2021) 'Ethiopia suspends aid groups for 'spreading misinformation'', available at https://www.theguardian.com/global-development/2021/aug/06/ethiopia-suspends-aid-groups-for-spreading-misinformation, accessed 16 March 2022.

Akande, D. and Emanuela-Chiara, G. (2019) 'Conflict-induced Food Insecurity and the War Crime of Starvation of Civilians as a Method ofWarfare The Underlying Rules of International Humanitarian Law', *Journal of International Criminal Justice,* 17 753-779.

Al-Bashiri, M. (2021) *Impacts Of The War On The Telecommunications Sector In Yemen,* Sanaa: Deeproot consulting.

Al-Jazeera (2022) 'Aid groups halt work in northwest Tigray after deadly strike: UN', available at https://www.aljazeera.com/news/2022/1/9/aid-agencies-suspend-work-in-northwest-tigray-after-deadly-strike, accessed 25 March 2022.

Ali, A. M. (2021) *Sudan Digital Rights Landscape Report,* Sussex: Institute of Development Studies.

Alston, P. (2019) *Report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, submitted in accordance with Human Rights Council resolution 35/19,* New York: UN.

Arraiza, J.-M. (2022) *From High-Risk Mass Identification Towards Inclusion and Protection. A Study on the Risks of Exclusion, Discrimination and Other Human Rights Concerns Related to the Design and Implementation of Digital Legal Identification Systems. Draft,* Geneva: United Nations.

Bahn, R., Al Kareem Yehya, A. and Zurayk, R. (2021) 'Digitalization for Sustainable Agri-Food Systems: Potential, Status, and Risks for the MENA Region', *Sustainability,* 13 (3223)

BBC (2001) 'US shuts down Somalia internet', available at http://news.bbc.co.uk/1/hi/world/africa/1672220.stm, accessed 9 March 2022.

Bothe, M., Partsch, K., Solf, W. (ed.) (2013) *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949. 2nd edition.* Leiden: Nijhoff.

Bryant, J., Holloway, K., Lough, O. and Willitts-King, B. (2020) *Bridging humanitarian digital divides during Covid-19,* HPG Briefing Note. London: Overseas Development Institute.

Burns, R. (2014) 'Moments of Closure in the Knowledge Politics of Digital Humanitarianism', *Geoforum,* 53 51–62.

Burton, J. (2020) '"Doing no harm" in the digital age: What the digitalization of cash means for humanitarian action', *International Review of the Red Cross,* 102 (913): 43–73.

CALP (2020) *CVA in COVID-19 contexts: guidance from the CaLP network,* Cash Learning Partnership.

CALP (2021a) *Assessment Of Financial Service Providers – CVA In Yemen,* CALP.

CALP (2021b) *Humanitarian Cash And Social Protection In Yemen. CaLP Case Study,* Sanaa: CALP.

Chonka, P. and Bakonyi, J. (2021) 'Precarious technoscapes: forced mobility and mobile connections at the urban margins', *Journal of the British Academy,* 9 (11): 67–91.

Clausen, M.-L. (2021) *Piloting Humanitarian Biometrics in Yemen,* MIDEAST POLICY BRIEF 1. Oslo: PRIO.

Cohen, N. (2018) '"Do no digital harm"', available at https://www.thenewhumanitarian.org/2018/10/17/do-no-digital-harm, accessed 5 April 2022.

Conley, B., De Waal, A., Murdoch, C. and Jordash, W. (eds.) (2022) *Accountability for Mass Starvation: Testing the Limits of the Law.* Oxford: Oxford University Press.

Coppi, G. and Fast, L. (2019) *Blockchain and distributed ledger technologies in the humanitarian sector,* HPG Commissioned Report. London: Overseas Development Institute.

Cosmas, K. (2014) 'The role of social media in the South Sudan crisis', available at https://www.peaceinsight.org/en/articles/role-social-media-south-sudan-crisis/?location=south-sudan&theme=culture-media-advocacy, accessed 12 March 2022.

Dannenbaum, T. (2021) 'Famine in Tigray, Humanitarian Access, and the War Crime of Starvation', available at https://www.justsecurity.org/77590/famine-in-tigray-humanitarian-access-and-the-war-crime-of-starvation/, accessed 28 March 2022.

De Waal, A. (1989) *Famine that Kills: Darfur, Sudan,* Oxford: Clarendon Press.

De Waal, A. (2018) *Mass Starvation. The History and Future of Famine,* Cambridge: Polity.

Devereux, S. (ed.) (2007) *The New Famines. Why famines persist in an era of globalisation.* London: Routledge.

Devidal, P. (2021) 'Cashless cash: financial inclusion or surveillance humanitarianism?', available at https://blogs.icrc.org/law-and-policy/2021/03/02/cashless-cash/, accessed 20 September 2021.

Diepeveen, S., Borodyna, O. and Tindal, T. (2022) 'A war on many fronts: disinformation around the Russia-Ukraine war', available at https://odi.org/en/insights/a-war-on-many-fronts-disinformation-around-the-russia-ukraine-war/?utm_source=ODI+updates&utm_campaign=e1c251893a-EMAIL_CAMPAIGN_2022_02_18_10_58_COPY_01&utm_medium=email&utm_term=0_1413423dcc-e1c251893a-76648964, accessed 21 March 2022.

Dinstein, Y. (2016) *The Conduct of Hostilities under the Law of International Armed Conflict. 3rd edition,* Cambridge: Cambridge University Press.

Duffield, M. (2018) *Post-Humanitarianism. Governing Precarity in the Digital World,* Cambridge: Polity Press.

Edkins, J. (2007) 'The criminalisation of mass starvations; from natural disaster to crime against humanity', in: Devereux, S. (ed.) *The New Famines; Why famines persist in an era of globalisation,* Abingdon: Routledge.

Elliott, R. (2020) 'Remote Data Collection in Northern Ethiopia: Tigray and Amhara', available at https://www.geopoll.com/blog/remote-data-collection-in-northern-ethiopia-tigray-and-amhara/, accessed 24 March 2022.

FAO (2009) *Declaration of the World Summit on Food Security,* Rome: Food and Agriculture Organisation.

FAO and WFP (2022) *Hunger Hotspots. FAO-WFP early warnings on acute food insecurity. February to May 2022 Outlook,* Rome: Global Network Against Food Crisis.

Gebremichael, T. (2022) 'Impact of the Internet Shutdown in Tigray', available at https://www.tghat.com/2022/02/24/impact-of-the-internet-shutdown-in-tigray/, accessed 28 February 2022.

Gisel, L., Rodenhauser, T. and Dormann, K. (2020) 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts', *International Review of the Red Cross,* 102 (913): 287–334.

Global Network Against Food Crisis (2022) *2022 Global Report on Food Crisis,* Rome: Food Security Information Network.

GRC (2021) 'Starvation Sanctions Digests', available at https://starvationaccountability.org/resources/digests/, accessed 26 May 2022.

GRC (2022) *The Starvation Training Manual: An International Framework Guide to the Law of Starvation. 2nd Edition,* The Hague: Global Rights Compliance.

GRC and Mwatana for Human Rights (2021) *Starvation Makers: The use of starvation by warring parties in Yemen,* The Hague: Global Rights Compliance.

GRC and WPF (2019) *The Crime of Starvation and Methods of Prosecution and Accountability. Accountability for Mass Starvation: Testing the Limits of the Law,,* Policy Paper. The Hague: Global Rights Compliance and World Peace Foundation.

GSMA (2021a) *Humanitarian cash and voucher assistance programmes in Ethiopia: Context analysis and capability assessment of the mobile money ecosystem,* GSMA.

GSMA (2021b) *Mobile money 4 CVA webinar presentation,* GSMA.

Hagmann, T., Musa, A. and M., W. (2021) *The political economy of aid data procurement and analysis in Somalia,* Itingen: Public Culture Lab HMBH.

Hamilton, Z. (2021) *COVID-19 and digital humanitarian action: Trends, risks and the path forward,* London: GSMA Mobile for Innovation.

Harvey, P. (2007) *Cash-based responses in emergencies,* HPG Report 24. London: Overseas Development Institute.

Henderson, I. (2009) *The Contemporary Law of Targeting, Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I,* Leiden: Nijhoff.

Hernandez, K. and Roberts, T. (2018) *Leaving No One Behind in a Digital World,* Brighton: Institute of Development Studies.

Holloway, K., Al Masri, R. and Afnan, A. Y. (2021) *Digital identity, biometrics and inclusion in humanitarian responses to refugee crises,* HPG Working Paper,. London: Overseas Development Institute.

Holloway, K. and Lough, O. (2021) 'Although shocking, the Rohingya biometrics scandal is not surprising and could have been prevented', available at https://odi.org/en/insights/although-shocking-the-rohingya-biometrics-scandal-is-not-surprising-and-could-have-been-prevented/, accessed 11 July 2021.

Hujale, M. (2020) 'Poor data protection could put lives at risk, say Somalia aid workers', available at https://www.theguardian.com/global-development/2020/dec/30/poor-data-protection-could-put-lives-at-risk-say-somalia-aid-workers, accessed 9 March 2022.

Human Rights Council (2018) *Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar**

Hutter, S. (2015) *Starvation as a Weapon: Domestic Policies of Deliberate Starvation as a Means to an End under International Law* Leiden: Nijhoff.

ICRC (2014) *Q&A and Lexicon on Humanitarian Access* Geneva: ICRC.

ICRC (2019) *International Humanitarian Law and Cyber Operations during Armed Conflicts. ICRC position paper,* Geneva: ICRC.

ICRC (2020) 'Q&A: Humanitarian operations, the spread of harmful information and data protection', *International Review of the Red Cross,* 102 (913): 27–41.

ICRC (2021) 'Cyberwarfare: does International Humanitarian Law apply?', available at https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law, accessed 27 April 2022.

IPC Global Partners (2021) *Integrated Food Security Phase Classification Technical Manual Version 3.1. Evidence and Standards for Better Food Security and Nutrition Decisions,* Rome: FAO.

Jacobsen, K. and Fast, L. (2019) 'Rethinking access: how humanitarian technology governance blurs control and care', *Disasters,* 43 (S2): S151–S168.

Jacobsen, K. and Steinacker, J. (2021) 'Contingency Planning in the Digital Age: Biometric Data of Afghans Must Be Reconsidered', available at https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/, accessed 17 September 2021.

Jaspars, S. (2018) *Food Aid in Sudan. A History of Power, Politics and Profit,* London: Zed Books.

Jaspars, S. (2019) *A Role for Social Nutrition in Strengthening Accountability for Mass Starvation?,* World Peace Foundation Occassional Paper 20, Boston: Tufts University.

Jaspars, S., Adan, G. and Majid, N. (2020) *Food and Power in Somalia: Business as Usual? A scoping study on the political economy of food following shifts in food assistance and in governance,* London: London School of Economics and Political Science.

Jaspars, S. and Sathyamala, C. (2021) *Digital Bodies and digitalised welfare: North-South linkages in the politics of food assistance and social welfare,* ISS Working Paper 687. The Hague: International Institute of Social Studies.

Jordash, W., Murdoch, C. and Holmes, J. (2019) 'Strategies for Prosecuting Mass Starvation'', *Journal of International Criminal Justice,* 17 (4)

Keen, D. (1994) *The Benefits of Famine. A political economy of famine and relief in south western Sudan 1983-89.,* Oxford: James Curry.

Lentz, E., Simmons, C., Gottlieb, G. and Maxwell, D. (2021) *Early Warning and Early Action for Increased Resilience of Livelihoods in the IGAD Region Report 3. Predictive Analytics and Machine Learning Approaches to Support EW-EA,* A Feinstein International Center Working Paper Feinstein International Center.

Macrae, J. and Zwi, A. (eds.) (1994) *War and Hunger. Rethinking international responses to complex emergencies.* London: Zed Books.

Maxwell, D. (2022) 'War in Ukraine is pushing global acute hunger to the highest level in this century', available at https://theconversation.com/war-in-ukraine-is-pushing-global-acute-hunger-to-the-highest-level-in-this-century-181414, accessed 29 April 2022.

Maxwell, D. and Hailey, P. (2021) 'Analysing Famine: The Politics of Information and Analysis in Food Security Crises', *Journal of Humanitarian Affairs,* 3 (1): 16–27.

Maxwell, D. and Majid, N. (2016) *Famine in Somalia. Competing Imperatives, Collective Failures, 2011-12,* London: Hurst and Co.

McQuillan, D. (2018) *AI will be used by humanitarian organisations – this could deepen neocolonial tendencies,* London: The Conversation.

Mebur, J. and Kwamy, I. (2019) 'Do no digital harm', available at https://www.gsma.com/mobilefordevelopment/blog/do-no-digital-harm/, accessed 5 April 2022.

Mock, N., Singhal, G., Olander, W., Pasquier, J. and Morrow, N. (2016) 'mVAM: A new contribution to the information ecology of humanitarian work', *Procedia Engineering,* 159 217 – 221.

Moore, J. (2020) 'Anatomy of an internet shutdown', available at https://restofworld.org/2020/sudan-revolution-internet-shutdown/, accessed 17 May 2022.

Muggah, R. (2022) 'Yemen's Parallel War in Cyberspace', available at https://foreignpolicy.com/2022/01/06/yemen-war-internet-media-houthis-iran-saudi-arabia/, accessed 6 May 2022.

Privacy International (2017) 'Social Media Intelligence', available at https://privacyinternational.org/explainer/55/social-media-intelligence, accessed 17 May 2022.

Privacy International and ICRC (2018) *The Humanitarian Metadata Problem: "Doing No Harm" In The Digital Era,* Geneva: Privacy International.

Radio Dabanga (2022) 'Intense attack on the social media accounts of Sudan activists', available at https://www.dabanga-sudan.org/en/all-news/article/intense-attack-on-the-social-media-accounts-of-activists-and-resistance-committees, accessed 2 March 2022.

Ranger, S. (2018) ‘What is cyberwar? Everything you need to know about the frightening future of digital conflict’, available at https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/, accessed 12 May 2022.

Reeves, B. (2017) ‘Online fake news and hate speech are fueling tribal ‘genocide’ in South Sudan’, available at https://theworld.org/stories/2017-04-25/online-fake-news-and-hate-speech-are-fueling-tribal-genocide-south-sudan, accessed 12 March 2022.

Rejali, S. and Heiniger, Y. (2020) ‘The Role Of Digital Technologies In Humanitarian Law, Policy And Action: Charting A Path Forward’, *International Review of the Red Cross,* 102 (913): 1-22.

Reuters (2022) ‘Yemen’s internet service returns after four-day outage following air strike’, available at https://www.reuters.com/world/middle-east/yemens-internet-service-returns-after-four-day-outage-following-air-strike-2022-01-25/, accessed 2 March 2022.

Sandoz, Y., Swinarski, C., Zimmerman, B. (ed.) (1987) Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Leiden: Nijhoff.

Sandvik, K., Gabrielsen Jumbert, M., Karlsrud, J. and Kaufmann, M. (2014) ‘Humanitarian technology: a critical research agenda’, *International Review of the Red Cross,* 96 (894): 219–242.

Sassòli, M. (2019) *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* Cheltenham: Edward Elgar.

Sassolli, S. (2017) *The Conduct of hostilities and International Humanitarian Law, Challenges of 21st Century Warfare,*

Schia, N. (2018) ‘The cyber frontier and digital pitfalls in the Global South’, *Third World Quarterly,* 39 (5): 821–837.

Sen, A. (1981) *Poverty and Famines. An Essay on Entitlement and Deprivation* Oxford: Clarendon Press.

Slim, H. (2015) *Humanitarian Ethics. A Guide to Morality of Aid in War and Disasters,* London: Hurst and Company.

Sojka, B., Harvey, P. and Slater, R. (2022) *Ukraine – can social protection be sustained and support a humanitarian response?,* Wolverhampton: University of Wolverhampton.

Spatz, B., Murdoch, C. and Windridge, O. (2022) ‘Sanctions as a Mechanism for Accountability for Starvation Crimes’’, in: Conley, B., De Waal, A., Murdoch, C. andJordash, W. (eds.) *Mass Starvation: Testing the Limits of the Law,* Oxford: Oxford University Press.

Spencer, S. (2021) *Humanitarian AI The hype, the hope and the future,* HPN Network Paper 85. Overseas Development Institute.

Stoddard, A., A., H. and Renouf, J. (2010) *Once Removed. Lessons and challenges in remote management of humanitarian operations for insecure areas,* London: Humanitarian Outcomes.

The Engine Room and Oxfam (2018) *Biometrics in the Humanitarian Sector,* Oxford: Oxfam.

Thomas, M. and Obrecht, A. (2016) *Mapping satellite imagery to aid humanitarian response: OpenStreetMap,* HIF/ALNAP Case Study. London: ODI/ALNAP.

Triffterer, O. and Ambos, K. (eds.) (2016) *The Rome Statute of the International Criminal Court: A Commentary. 3rd edition.* Oxford: Beck/Hart.

UNICEF (1990) *Strategy for Improved Nutrition of Children and Women in Developing Countries,* New York: United Nations Children’s Fund.

Von Carnapp, T. (2022) ‘Ethiopia Rural Market Monitor’, available at https://sites.google.com/view/tillmann-von-carnap/ethiopia-rural-market-monitor?authuser=0, accessed 31 March 2022.

Weitzberg, K., Cheesman, M., Martin, A. and Schoemaker, E. (2021) ‘Between surveillance and recognition: Rethinking digital identity in aid’, *Big Data & Society,*

WFP (2016a) ‘MVAM the blog’, available at https://mvam.org/page/14/, accessed 16 March 2022.

WFP (2016b) *WFP SCOPE. Know them better, to serve them better,* Rome: World Food Programme.

WFP (2021) *Internal Audit of SCOPE WFP’s Digital Management of Beneficiaries,* Rome: World Food Programme.

WFP (2022a) *Emergency Food Security Assessment Tigray Region, Ethiopia,* Addis Ababa: World Food Programme.

WFP (2022b) ‘Hunger map’, available at https://hungermap.wfp.org/, accessed 23 March 2022.

WFP (2022c) *Summary report on the strategic evaluation of WFP’s use of technology in constrained environments,*

WPF (2021) *Starving Tigray: How Armed Conflict and Mass Atrocities Have Destroyed an Ethiopian Region’s Economy and Food System and Are Threatening Famine,* Boston: World Peace Foundation.

WORLD PEACE FOUNDATION

LSE IDEAS

PeaceRep
Peace and Conflict
Resolution Evidence
Platform