



# Uses of digital technologies in managing and preventing conflict

Luke Kelly

University of Manchester

17 May 2019

## Question

How are digital technologies used to prevent, manage or address violent conflict and promote stabilisation and peacebuilding?

- What are the positive effects of using ICTs in this area?
- In what ways have development programmes and their beneficiaries been affected by the malign use of digital ICT in conflict contexts (including in the context of hybrid warfare) and how can they protect themselves?

## Contents

1. Summary
2. Use of ICTs in violence prevention, stabilisation and peacebuilding
3. Malign use of ICTs
4. References

---

*The K4D helpdesk service provides brief summaries of current research, evidence, and lessons learned. Helpdesk reports are not rigorous or systematic reviews; they are intended to provide an introduction to the most important evidence related to a research question. They draw on a rapid desk-based review of published literature and consultation with subject specialists.*

*Helpdesk reports are commissioned by the UK Department for International Development and other Government departments, but the views and opinions expressed do not necessarily reflect those of DFID, the UK Government, K4D or any other contributing organisation. For further information, please contact [helpdesk@k4d.info](mailto:helpdesk@k4d.info).*

# 1. Summary

This query looks at the role of ICTs in preventing, managing and promoting peacebuilding and stabilisation. It also considers the threats to humanitarian programmes brought by ICTs.

Information Communication Technologies (ICTs) are increasingly prevalent across the developing world and as such are being used in a variety of ways to prevent, prevent or address violence conflict. ICTs can be defined as 'electronic equipment and applications that are used to find, analyse, create, communicate, disseminate and use information' (HD, 2019). The ICTs surveyed in this paper include mobile phones, the internet, social media platforms such as Whatsapp, Facebook and Twitter, satellites, and GIS mapping applications, and the crowdsourcing of information through these platforms. A large number of applications have been developed to gather, map and disseminate data on peace and conflict. These include the Ushahidi platform, first developed in Kenya in 2008 and used widely since.

Overall, ICTs can help manage and prevent conflict, and build peace, in the following ways:

- Identifying and mapping hate speech and rumours;
- Countering hate speech and rumours;
- Identifying and mapping risks to livelihood or other likely causes of conflict;
- Collating and analysing citizens' perceptions of risk and conflict;
- Mapping violent incidents;
- Tracking armed groups;
- Providing early warning;
- Identifying examples of peaceful behaviour.

ICTs can help gather a large volumes of information on peace and conflict that can be used to track violence and its causes. ICTs are seen to be less useful in gathering in-depth interview-style information. ICTs also have applications in preventing conflict through information or positive messaging. A number of initiatives have been undertaken by NGOs, but there are few comprehensive evaluations.

Broadly speaking, ICTs can be used in 'vertical' and 'horizontal' configurations. In the former, ICTs are used by governments to gather and analyse data from populations, or to disseminate messages. In the latter, ICTs such as mobile phones and social media are used by citizens and civil society groups to spread information between citizens, or to the government. The use to which ICTs are put also depends on models of conflict prevention and peacebuilding, which range from tracking and halting insurgent groups by force, to surveying risks and seeking to empower ordinary citizens.

The literature suggests that programmes using ICTs should pay close attention to contextual factors such as the use of technology, the population's technological literacy, and the data analysis capacities of the implementing organisation.

Humanitarian organisations have as yet developed few specific techniques to protect themselves from the malign use of ICT. Suggested safety measures include the use of data protection principles, risk assessments, and more advocacy of 'humanitarian space'.

A number of research centres looking into the uses of ICT in peace and conflict prevention have been started. They include research centres at Stanford, Harvard and MIT, Everyday Peace Indicators at Georgetown University, the ICT4Peace Foundation, and PeachTech Lab (Firchow,

Martin-Shields, Omer, & Ginty, 2017). This review drew on academic and grey literature. This was largely gender-blind. Academic and policy literature focuses on understanding how ICTs affect the dynamics of conflict, humanitarian programmes, and potential new uses of ICTs. Given the fast pace of innovation, some areas are not thoroughly evaluated.

## 2. Use of ICTs in violence prevention, stabilisation and peacebuilding

### 2.1 General communication

**ICT is used by most humanitarian and development organisations to gather and share information.** Researchers have found that mobile phones can supply useful data for programmes. Peacebuilders use mobile phones to 'collect near real-time monitoring data about outcomes and results of programme activities', especially in remote areas. Uses include checking whether programmes have been implemented as agreed, and learning based on how the programmes fared (Corlazzoli, 2014). Mobile phones can serve as a way for researchers to save data, can be used to ask questions of participants, and can be part of 'crowdsourcing systems' by which data is shared, and can be used to conduct interviews and surveys (Perera, 2017).

### 2.2 Collect data on conflict or peacebuilding events

ICT has a number of applications in data gathering and data presentation that can aid the management and prevention of conflict. Mobile phones and internet platforms are being used to survey risk in areas undergoing conflict or at risk of conflict. Military peacekeeping missions have used satellite mapping on their missions to see the movements of troops or peoples.

**Satellite and drone mapping technology can provide images of difficult-to-reach conflict-affected areas.** While limited by factors such as cloud cover, this method can provide information otherwise unattainable. The information gathered through such mapping can take time to process. Satellite mapping also needs to be analysed, as 'geospatial information without a corresponding political narrative can be unhelpful or even misleading, misrepresenting the timeline of events and skewing causal explanations for conflicts' (Convergne & Snyder, 2015)

The UN's Geospatial Information Section (UN GIS), OCHA's Relief Web Maps, or UNOSAT all provide maps or analysis of geographic data. Moreover, 'open-source and crowd-sourced tools such as Airbus Defence and Space, Global Incident Map, Jane's Satellite Imagery Analysis, Liveuamap, MDA Geospatial Services, and Ushahidi provide important low-cost alternatives' for smaller organisations (HD, 2019).

Satellite mapping is being used in the following ways by peacekeepers:

- the demarcation and enforcement of international boundaries;
- support for the negotiation and implementation of ceasefire and peace agreements;
- stabilization and violence prevention operations; electoral assistance;
- the protection of civilians;
- human rights monitoring;
- support for the extension of state authority and the rule of law;
- the provision of humanitarian assistance.

In situations where borders or facts on the ground are subject to debate, a UN-supplied map can ‘equalize information held by different stakeholders as a prerequisite to better dialogue, decision making and monitoring.’ For example, satellites were used to create impartial maps in the Dayton Peace Accords between Sudan and South Sudan in 2011 (HD, 2019).

By mapping the location and frequency of violence, it can be used to calculate force to space ratios for peacekeepers, as in the 2012 election violence in Timor-Leste. Satellite images can also be used to detect attacks soon enough for peacekeepers to intervene (Convergne & Snyder, 2015, p. 566). In Syria and Yemen, GPS location data on hospitals and schools has been given to the warring parties who can then make sure these buildings are not attacked, as part of a process called deconfliction.<sup>1</sup>

## 2.3 Collect data on conflict and stability risks for early warning analysis

**ICTs can be used to gather data on, and map, potential triggers for conflict such as resource shortages or movements of people.** Data on violence is being analysed to understand patterns and causes of violence. Predictive peacekeeping is defined as ‘a range of analytic tools and peacekeeping practices that serve to forecast where and when armed violence will take place, combined with changes in peacekeeping leadership decision making — in particular deployment of peacekeeping staff — based on those forecasts’. The UN’s Situational Awareness Geospatial Enterprise (SAGE) database of events is designed to facilitate machine learning to detect patterns and predict conflict. Machine learning can analyse patterns, rarely than following pre-set rules, and can therefore help to show how ‘events and developments combine to affect outcomes’. For predictive peacekeeping to be successful, both informed theories on the likely risk factors, and meaningful data are required. In the case of Darfur, highly local data such as livestock thefts or splits in rebel groups are good predictors and are well-covered by the Joint Mission Analysis Centre (JMAC) database (Duursma & Karlsrud, 2019).

Discussing the role of data in peacebuilding, Mac Ginty argues that ‘information systems...seem geared to recording incidents rather than processes’ and thus miss the ‘chronic nature’ and structural causes of violence (2017, p. 699). He therefore points to the importance of human-centred data in everyday contexts, for which ICTs are less useful. While ICTs can help gather survey information from remote populations at little cost, it should not supplant traditional human-centred forms of knowledge-gathering. Predictive peacekeeping therefore requires significant resources in both collecting and analysing data and looking for causal relationships.

The **Crisis and Recovery Mapping and Analysis project (CRMA) project** run by UNDP Sudan has sought to map risks affecting Sudan and South Sudan and involve the local population. The project gathered perceptions on threats through community workshops, facilitated by government officials, which were plotted on a GIS database tool. Two early warning systems were piloted based on this data, including the **Conflict Early Warning and Response Unit (CEWERU)**. Conflict incidents with their geographical location can be reported by local officers and added to the database. The early warning reports are analysed each month by a

---

<sup>1</sup> <https://www.thenewhumanitarian.org/analysis/2018/11/13/what-humanitarian-deconfliction-syria-yemen>

technical team at the state level. The success of such projects depends on whether the technology can make 'actionable data'. This requires it to be linked to existing local capacities, for analysis as well as action (Larrauri, 2013).

**Where data is being crowdsourced, it is important to tailor programmes according to the population's capacities and access to technology.** In Kyrgyzstan, initiatives run by UNDP and USAID, the EC and the UNHCR have failed as early warning systems. A 2010-11 UNDP and UN Women-funded early warning system failed because many of the rural women expected to provide the warnings by SMS were semi-literate and struggled to use the technology. Sending analysts to the field to verify information or explain technology is costly and delays the information (Mateeva, 2013). In areas with low mobile phone and internet coverage, paper-based systems may be more appropriate. Summarising the lessons from several cases studies, Mancini and O'Reilly (2013) emphasise the importance of using ICT to 'bolster existing local capacities' or alongside technologies actually being used.

**The use of technology to gather and disseminate data should therefore be determined by local capacity.** Several studies criticise 'supply-driven' use of ICTs. Some tools, such as interactive maps, may require training for users and local implementing partners. Although ICT use across the world, including the developing world, is rising, not all populations are equally connected to these networks, leading to 'digital divides' within and across countries. The regulatory environment for internet, telecoms and media, and the level of connectedness, are important factors. It is therefore important to consider the most appropriate technologies for a given context. In some cases, non-digital technology may be more effective

## 2.4 Collect data on citizen perceptions

**Social media produces large volumes of data on a population's views, which can be used to predict instability and conflict.** The Carter Centre Syria Conflict Mapping Project aims to provide analysis of 'feelings and thoughts' of a population (Corlazzoli, 2014). Researchers in Mexico have analysed millions of tweets to assess attitudes to the government, drug cartels and the media in Mexico. They have identified 'civic media curators...responsible for a disproportionate number of violence-related real-time tweets'. Another researcher has analysed new and old media to show the 'micromechanisms of drug-related violence' (Muggah & Diniz, 2013). The value of such analyses is that they can produce a lot of data in real time to give peacebuilders an image of the situation (Corlazzoli, 2014). However, such large aggregations of data can include biases and inaccuracies, not least because of unequal levels of access to technology (HD, 2019; Mac Ginty, 2017).

Several studies point to the limited amount of nuance and contextual data that can be derived from SMS or internet-based surveys and **advise the continued use of face-to-face methods for in-depth data collection.** Based on fieldwork in the DRC, Perera argues that SMS surveys can 'at best be a supplementary form of conflict data' and points to the continued need for fieldwork to produce detailed, contextualised knowledge. Aside from a lack of verification, remote surveys via SMS or other methods often only produced brief, factual answers (Perera, 2017). Mac Ginty has looked at the use of SMS surveys in parts of Cape Town that are dangerous to access and notes the difficulty of getting contextual information (Firchow & Mac Ginty, 2017). These scholars emphasise the limits qualitative data gathered through ICT, the need to use it alongside traditional, human-centred methods, and the importance of human networks and personalities (Mac Ginty, 2017).

## 2.5 Collect data on armed groups

ICTs can be used by military peacekeepers or security forces to **gather intelligence on rebel groups or criminal groups** (Berman, Felter, & Shapiro, 2018; Muggah & Diniz, 2013). Recent analysis of the United States' military data from Iraq has sought to understand how ICT data can be effective in fighting insurgencies. ICTs can be used to gather two forms of intelligence by military peacekeeping or pacification missions. Signals intelligence (SIGINT) is the term to describe information on the planned operations of armed groups, derived from interception communications or assessing patterns of activity. HUMINT is human intelligence from the population at large, including tip-offs on armed group activity as well as perceptions of risks and information on relations between groups and the population.

It is important to consider not just the technologies used to gather data, but also the **costs and benefits of providing information**, and the **relationship between those informing and peacekeepers**. ICTs have been used to track violence in Latin America, the region with the highest rates of organised and interpersonal violence in the world. Partly because of a legacy of authoritarian government, security forces have led the way in developing ICT platforms to trace gangs and violence. Police forces in countries such as Brazil, Colombia and Mexico have developed platforms to gather and analyse large amounts of data from surveillance systems and police and citizen reporting using models developed in the US. Infocrim in Sao Paulo has been credited with a fall in homicides from 12,800 to 7,200 in the period 1999-2005, and has been copied across the continent. The Rio de Janeiro Smart City programme includes banks and technology firms as partners (Muggah & Diniz, 2013).

**High rates of ICT use in the region have seen a number of horizontal approaches to gathering this data, led by citizens or NGOs.** Citizen-reporting systems and blogs have been used to produce data on violence, particularly in countries where the press self-censors or citizens fear violent reprisals if they report to authorities. Many of these initiatives have been started by NGOs or citizens. These include blogs reporting on drug gang violence and information sharing on state-led pacification measures. While these initiatives bring benefits such as a potentially wide pool of informers and inclusivity, they also bring risks of false information and vigilante justice. However, there is little analysis of the efficacy of these measures in the Latin American context (Muggah & Diniz, 2013, p. 38).

While vertical approaches have been successful in enhancing state security goals, horizontal approaches have the potential to improve the accountability of state security forces and work effectively in situations where the police or gangs inspire fear (Muggah & Diniz, 2013).

## 2.6 Counterinsurgency

**ICT can be used to combat armed groups and prevent attacks.** Shapiro and Siegel (2015) note the apparent paradox that ICTs in conflict situations can 'make it easier for anti-government actors to coordinate and solve collective action problems, but they can also help government forces repress activism'. They use game theory to model this issue and conclude that ICTs will help a government suppress an insurgency if they increase the government's ability to report the group's activities more than the ability of the group to retaliate.

Analysing mobile phone coverage, American SIGINT data in Iraq, and examples from Africa and the Philippines, Berman and Shapiro argue that **more ICT coverage benefits the government in asymmetric wars, whereas in symmetrical wars it tends to benefit rebel groups**. Internet and mobile phone networks allow rebel groups to co-ordinate attacks and detonate bombs. However, the advantages of more intelligence are greater for governments already enjoying a military advantage: they can intercept rebel communications and can also get tip-offs from the civilian population, which allows them to find the rebels and benefit from their advantage in force. Conversely, without communication networks, it is much more difficult and dangerous for civilians to inform on rebel groups, who can therefore hide within the civilian population more easily (Berman and Shapiro, 2018). Because of these factors, conflict parties such as Boko Haram and the Nigerian government, the Taliban, and those involved in the Yemeni and Syrian wars, have shut down or reduced access to communications technology at various times. By contrast, the US military sought to install cell phone towers in Iraq partly to help fight insurgencies.

## 2.7 Collect data on hate speech and rumours

Hate speech is seen to be a driver of conflict, and to be driven by ICTs. A number of platforms were developed to track hate speech following the 2008 post-election violence in Kenya:

- **Ushahidi** was established in 2008 to map election violence. It gets data from Facebook, Twitter and SMS and works with civil society actors. It has been used in many other contexts since.
- **Uchaguzi** is a telephone-based system. Users send an SMS about incidents of violence. It is verified and sent to the authorities. As it has a toll-free number, it is useful in poor areas with no internet.
- **Uwiano Platform for Peace** was launched in 2010 by the government and UNDP and included NGOs such as PeaceNet Kenya. It provides online tracking tools and citizens can send an SMS to report an incident.
- **Umati** is a project established in 2013 to monitor hate speech on the internet and input it into a database and map.
- On Facebook, **Elections Iwitness Kenya** and **Kenya Elections 2013** were used to share experiences of election malpractice or violence.
- **Sisi Ni Amani** was a programme to improve civic education and prevent violence using SMS messaging in the 2013 election.
- **Una Hakika ('Are you sure?')**, established in 2017, is an information service that tries to check potentially dangerous rumours, using mobile phones.

According to Mutahi and Kimari, 'The main challenge in using social media to forecast violence is ensuring the veracity and authenticity of the information gathered before it leads to violence' (Mutahi & Kimari, 2017b, p. 22). Although rating it a success, an ALNAP evaluation of Uchaguzi noted the difficulties brought by crowdsourcing information, and the need for filters and staff to verify information sent remotely (*Uchaguzi: A Case Study Executive Summary*, n.d.).

## 2.8 Counter hate speech and rumours

ICTs can be used to **counter false rumours, disseminate peaceful messages, and provide a platform for peace-promoting initiatives**. They work on the basis of the Ceasefire programme in Chicago that violence is a transmittable disease (Larrauri & Kahl, 2013). There are examples of ICTs being used successfully to counter hate speech and false rumours. However, these platforms may also be reliant on pre-existing networks of trust or reliable institutions.

Although ICTs can be used to trace hate speech, it is hard to define hate speech in law and governments often struggle to prosecute sites registered abroad. Moreover, the prosecution of hate speech can have the unintended consequence of making it more rather than less visible (Mutahi & Kimari, 2017b, p. 23).

**More evaluation of programmes to counter false rumours or hate speech is needed.** An evaluation of Sisi Ni Amani's work, based on a survey sampling its users, was conducted by Sisi Ni Amini and researchers from the University of Pennsylvania. It was found that civic education messages were useful to those receiving them. The study also indicated that participants thought the messages had a calming effect. It suggested the more specific messages offered by the platform were more effective than many of the generic peace messages circulated around the elections. However, the study did not include non-subscribers to the service or offer comparison with other ICT messages available to Kenyans and therefore cannot show why the network was trusted (Shah & Brown, 2014).

Other studies point to **the importance of existing networks of kinship, creed and language** in propagating rumours as well as countering them. For instance, a study looked at three civil society organisations in South Africa, Tanzania and Uganda using ICT to resolve conflict. It was found that although ICTs could help communicate messages at low cost, success often depended on relationship building and local partners who had already developed trust in affected communities (Morrison, 2016).

Seeking to explain the success of ICT platforms in reducing violence in Kenya, Martin-Shields (2013) argues that ICTs **can help reduce violence in situations of information asymmetry**, where elites are seeking to stoke group rivalry. He proposes four contextual factors needed for ICTs to be able to reduce violence: that violence is not preferred by the population, but rather a consequence of elite-'manufactured fear and perceived risk'; that violence occurs during particular times, such as after elections; that ICT use is widespread and mechanisms of reporting are known; and that there is buy-in from the government, UN or another actor to enforce conflict prevention measures. In areas where institutions are weaker or ICT networks are less prevalent such as the Democratic Republic of Congo, ICT platforms are unlikely to be effective.

Where ICTs are used to counter false rumours and hate speech, ICT use needs to be **matched by appropriate capacity for verifying and analysing data**. When used to report incidents or false rumours, organisations can quickly become swamped by submissions from the public. It is therefore important to be able to verify the data gathered so it is actionable. Such programmes also depend on context and may only work where information asymmetry is the cause of conflict. While programmes in Kenya are seen to have been effective, more research is needed to evaluate them.



## 2.9 Engage citizens

Scholars of peacebuilding debate the efficacy of **peace processes built by outside actors versus those involving local actors**. The use of ICTs to prevent conflict or promote peace depends on the approach taken, and the context of the conflict, as much as the technology used. In all contexts, however, ICTs can gather a greater volume of data, often at lower cost, and can sometimes reach more remote areas. Several scholars also point to the importance of understanding the local dynamics of peace and point to the value of tracing the views and actions of ordinary people not involved in the conflict as potential barriers to its spread (Heinzelmann et al., 2011; Mac Ginty, 2017). From this perspective, ICTs such as mobile phones and social media with a wide reach have a significant potential to produce useful data for analysis of the dynamics of conflict.

**ICTs can be a cost-effective way to involve ordinary people in peace processes.** For example, in Colombia during the negotiations between the government and FARC a website was built to allow submissions from the public. In Libya, the Centre for Humanitarian Dialogue built an online platform to garner comments on the UN Action Plan for the consultation phase. The Donbass Dialogue is an online platform where both sides of the Russia-Ukraine conflict can submit issues of concern anonymously. In all of these examples, ICTs have allowed inclusion of more of the population. However, the method risks sampling bias in favour of the younger and more affluent citizens more likely to be online. The large volume of responses – 67,371 in Colombia – need to be sorted and managed appropriately. Finally, such an approach also risks being a 'superficial form of inclusion' (HD, 2019).

**ICT can be used in more or less participatory ways in peacebuilding.** For example, in post-civil war Sri Lanka the government, keen to marginalise the defeated rebel group (the LTTE), banned social media and has sought to suppress information on humanitarianism and development in the country. Peacekeeping organisations can also use ICTs to disseminate information about their work, such as the UNDP's use of social media in Cyprus, although this can be 'static' and lack interactivity. In a number of other contexts, ICTs have been used to encourage grassroots participation in peacebuilding. However, the authors emphasise that grassroots use of ICTs 'does not necessarily iron out power imbalances', but can, in some cases, have the opposite effect. ICTs can be tools for a more inclusive peace process, but do not guarantee it as access is not always uniform across a population (Tellidis & Kappler, 2016).

**Maps can be used in a number of participatory ways.** Heinzelmann, Brown, & Meier (2011) put forward the concept of 'peace mapping' as a way to show 'ordinary people and their efforts' to build peace, and legitimise these by publicity. It can also strengthen individuals' resolve to find ways to get involved in peace and asks them to submit information about themselves and their skills via SMS or the internet. The peace map is based on the theory of the Third Side: that those not involved in violent conflicts can be important agents in preventing and delegitimising conflicts, especially when their options and their example are publicised (Corlazzoli, 2014; Heinzelmann et al., 2011). However, the peace map has not been implemented or evaluated so we cannot judge its efficacy.

## 3. Malign use of ICTs

### 3.1 Mobilisation of violence

#### **Research points to the role of ICTs in triggering and facilitating violence in populations.**

Writing about the spread of ethnic conflict, Weidmann (2015) shows that information about violence 'triggers strategic learning and demonstration effects in subnational conflict actors which may increase the likelihood that these actors ultimately resort to violence' (See also: Mutahi & Kimari, 2017a; Pierskalla & Hollenbach, 2013). In this context, ICTs are one link that can transmit information and therefore encourage or discourage violence. They have been used to spread misinformation, disinformation and hate speech in several contexts. ICTs transmit beliefs and behaviours by tapping into psychological and neurological as well as political factors (Brown & Livingston, 2018). As ICTs such as mobile phones and social media work peer to peer, and across borders, they can act as a relatively novel another vector of transmission of beliefs and tactics likely to lead to violence for which preventions strategies have not been fully developed. For example, ICTs are seen to have spread false rumours and hate speech in Kenya around the 2008 elections.

### 3.2 Cyberwarfare, cybercrime and espionage

#### **The use of ICT in programmes and by conflict parties brings a number of risks to humanitarian organisations.**

Hybrid warfare increasingly includes the use of information technology, and can bring a number of risks to peacebuilders and development organisations. ICTs can be used in to disrupt and subvert humanitarian organisations. Cyber-crime and cyber warfare, defined as 'any hostile measures against an enemy designed 'to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer', are increasing risks. A UNOCHA report lists several risks this brings to humanitarian organisations:

- Targeting of beneficiaries' personally identifiable data, as well as community identifiable data, for criminal or political purposes.
- Nuisance attacks on websites or social media accounts.
- Dissemination of false rumours, particularly using hijacked humanitarian accounts.
- Monitoring and surveillance, including for targeting purposes;
- Internet shutdowns;
- Competition for control of critical internet resources;
- Infrastructure sabotage or disruption.

(HD, 2019; UN OCHA, 2014)

According to the UNOCHA report, **the challenges brought by cybercrime require greater investment in risk analysis and information security measures.** With regards to the risk of personal data being stolen, and used to target individuals or communities, it recommends data protection and privacy assessments, and the anonymisation and redaction of personal data used in programmes. It warns against the mosaic effect, whereby multiple datasets can be overlain to get round anonymisation. It recommends that workers are given basic training in cybersecurity, and risk assessments included in programmes. It also recommends advocacy for legal frameworks for information sharing in emergencies, and for 'humanitarian space' to discourage the hacking of humanitarian organisations (UN OCHA, 2014).

## 4. References

- Berman, E., Felter, J. H., & Shapiro, J. N. (2018). *Small wars, big data : the information revolution in modern conflict*. Princeton, New Jersey: Princeton University Press.
- Brown, R., & Livingston, L. (2018). a new approach to assessing the role of technology in spurring and mitigating conflict: evidence from research and practice. *Journal of International Affairs*, 71(Special). Retrieved from <https://jia.sipa.columbia.edu/new-approach-assessing-role-technology-spurring-and-mitigating-conflict-evidence-research-and>
- Convergne, E., & Snyder, M. R. (2015). Making Maps to Make Peace: Geospatial Technology as a Tool for UN Peacekeeping. *International Peacekeeping*, 22(5). <https://doi.org/10.1080/13533312.2015.1094193>
- Corlazzoli, V. (2014). *ICTs for Monitoring and Evaluation of Peacebuilding Programmes*. Retrieved from <https://www.alnap.org/system/files/content/resource/files/main/ccvri-ssp-ict-and-me-final.pdf>
- Duursma, A., & Karlsrud, J. (2019). Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations. *Stability: International Journal of Security and Development*, 8(1), 1–19. <https://doi.org/10.5334/sta.663>
- Firchow, P., & Mac Ginty, R. (2017). Including Hard-to-Access Populations Using Mobile Phone Surveys and Participatory Indicators. *Sociological Methods and Research*. <https://doi.org/10.1177/0049124117729702>
- Firchow, P., Martin-Shields, C., Omer, A., & Ginty, R. Mac. (2017). PeaceTech: The Liminal Spaces of Digital Technology in Peacebuilding. *International Studies Perspectives*, 18, 4–42. <https://doi.org/10.1093/isp/ekw007>
- HD, U. and. (2019). *Digital Technologies and Mediation in Armed Conflict*. Retrieved from <https://peacemaker.un.org/sites/peacemaker.un.org/files/DigitalToolkitReport.pdf>
- Heinzelmann, J., Brown, R., & Meier, P. (2011). Mobile technology, crowdsourcing and peace mapping: new theory and applications for conflict management. In M. Poblet (Ed.), *Mobile Technologies for Conflict Management: Online Dispute Resolution, Governance, Participation* (pp. 39–53). [https://doi.org/10.1007/978-94-007-1384-0\\_4](https://doi.org/10.1007/978-94-007-1384-0_4)
- Herbert, S., Higazi, A., and Owen, Olly. (2019). *Farmer-pastoralist conflicts in Nigeria: A stakeholder mapping*, GSDRC Working Paper, forthcoming.
- Larrauri, H. P. (2013). New Technologies and Conflict Prevention in Sudan and South Sudan. In F. Mancini (Ed.), *New Technology and the Prevention of Violence and Conflict* (pp. 71–86). New York: International Peace Institute.
- Larrauri, H. P., & Kahl, A. (2013). Technology for Peacebuilding. *Stability: International Journal of Security & Development*, 2(3), 1–15. <https://doi.org/10.5334/sta.cv>
- Mac Ginty, R. (2017). Peacekeeping and Data. *International Peacekeeping*, 24(5), 695–705. <https://doi.org/10.1080/13533312.2017.1383561>
- Mancini, F. (ed. . (2013). *New Technology and the Prevention of Violence and Conflict*. Retrieved from [www.ipinst.org](http://www.ipinst.org)

- Mancini, F., & O'Reilly, M. (2013). Conclusion: New Technology in Conflict Prevention. In F. Mancini (Ed.), *New Technology and the Prevention of Violence and Conflict* (pp. 87–92). New York: International Peace Institute.
- Martin-shields, C. (2013). Inter-ethnic Cooperation Revisited: Why mobile phones can help prevent discrete events of violence, using the Kenyan case study. *Stability: International Journal of Security & Development*, 2(3), 58. <https://doi.org/10.5334/sta.cu>
- Mateeva, A. (2013). Conflict Cure or Curse? Information and Communication Technologies in Kyrgyzstan. In F. Mancini (Ed.), *New Technology and the Prevention of Violence and Conflict* (pp. 56–70). New York: International Peace Institute.
- Muggah, R., & Diniz, G. (2013). Using Information and Communication Technologies for Violence Prevention in Latin America. In *New Technology and the Prevention of Violence and Conflict* (pp. 28–41). New York: International Peace Institute.
- Mutahi, P., & Kimari, B. (2017a). The Impact of Social Media and Digital Technology on Electoral Violence in Kenya. In *Institute of Development Studies* (Vol. 2017).
- Perera, S. (2017). To Boldly Know: Knowledge, Peacekeeping and Remote Data Gathering in Conflict-Affected States. *International Peacekeeping*, 24(5), 803–822. <https://doi.org/10.1080/13533312.2017.1383566>
- Pierskalla, J. H., & Hollenbach, F. M. (2013). Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa. *American Political Science Review*, 107(2). <https://doi.org/10.1017/S0003055413000075>
- Shah, S., & Brown, R. (2014). *Programming for Peace: Sisi Ni Amani Kenya and the 2013 Elections*. Retrieved from <http://www.global.asc.upenn.edu/app/uploads/2014/12/SisiNiAmaniReport.pdf>
- Shapiro, J. N., & Siegel, D. A. (2015). Coordination and security: How mobile communications affect insurgency. *Journal of Peace Research*, 52, 312–322. <https://doi.org/10.1177/0022343314559624>
- Tellidis, I., & Kappler, S. (2016). Information and communication technologies in peacebuilding: Implications, opportunities and challenges. *Cooperation and Conflict*, 51(1), 75–93. <https://doi.org/10.1177/0010836715603752>
- Uchaguzi: A Case Study Executive Summary*. (n.d.). Retrieved from <https://www.alnap.org/system/files/content/resource/files/main/uchaguzi-121024131001-phpapp02.pdf>
- UN OCHA. (2014). *Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies*. Retrieved from [www.unocha.org](http://www.unocha.org).
- Weidmann, N. B. (2015). Communication networks and the transnational spread of ethnic conflict. *Journal of Peace Research*, 52, 285–296. <https://doi.org/10.1177/0022343314554670>

## Acknowledgements

We thank the following experts who voluntarily provided suggestions for relevant literature or other advice to the author to support the preparation of this report. The content of the report does not necessarily reflect the opinions of any of the experts consulted.

- Nils B Weidemann, University of Konstanz
- Roger Mac Ginty, Durham University
- Stefanie Kappler, Durham University
- Ioannis Tellidis, Kyung Hee University
- Rachel Brown, Project Over Zero
- Helena Puig Larrauri, Build Up

## Suggested citation

Kelly, L. (2019). *Uses of digital technologies in managing and preventing conflict*. K4D Helpdesk Report. Brighton, UK: Institute of Development Studies.

## About this report

*This report is based on six days of desk-based research. The K4D research helpdesk provides rapid syntheses of a selection of recent relevant literature and international expert thinking in response to specific questions relating to international development. For any enquiries, contact [helpdesk@k4d.info](mailto:helpdesk@k4d.info).*

*K4D services are provided by a consortium of leading organisations working in international development, led by the Institute of Development Studies (IDS), with Education Development Trust, Itad, University of Leeds Nuffield Centre for International Health and Development, Liverpool School of Tropical Medicine (LSTM), University of Birmingham International Development Department (IDD) and the University of Manchester Humanitarian and Conflict Response Institute (HCRI).*

*This report was prepared for the UK Government's Department for International Development (DFID) and its partners in support of pro-poor programmes. It is licensed for non-commercial purposes only. K4D cannot be held responsible for errors or any consequences arising from the use of information contained in this report. Any views and opinions expressed do not necessarily reflect those of DFID, K4D or any other contributing organisation. © DFID - Crown copyright 2019.*

