PEIC

PROTECT EDUCATION IN INSECURITY AND CONFLICT

حماية التعليم في ظروف النزاع وانعدام الأمن

HUMANITARIAN TECHNOLOGY AND THE MONITORING AND REPORTING OF ATTACKS ON EDUCATION

PEIC PAPER

January 2015

HUMANITARIAN TECHNOLOGY AND THE MONITORING AND REPORTING OF ATTACKS ON EDUCATION

BY: JANE KALISTA
International Consultant
Protect Education in Insecurity and Conflict (PEIC)
Education Above All Foundation

January 2015

Designed and printed by Digital Print House (DPH) - QF Publishing Center (QFPC)

CONTENTS

FOREWORD

Over recent years, the 'attacks on education' agenda has faced the challenge of enhancing the quality and quantity of data in order to fill the information and knowledge gaps concerning this phenomenon, harness information for purposes of advocacy and use available data to inform policy-making and programming. In particular, the *Education under Attack* publications (UNESCO 2007, UNESCO 2010, GCPEA 2014) have played a vital role in efforts to improve awareness and understanding of attacks on education occurring in dozens of countries around the world, drawing upon newspaper and other media sources, UN reports, academic research and studies undertaken by civil society organisations, including human rights groups. These publications relied largely upon secondary rather than primary sources of data and also adopted a retrospective approach rather than one seeking to capture 'current' data about ongoing events. There are understandable reasons for these orientations, including the unavailability of data in many conflict-affected situations, problems of verification, and the fact that sometimes the full and accurate details of specific incidents emerge only after the passage of time. The challenge of finding ways to overcome these and other difficulties or to supplement customary data gathering processes has stimulated interest in improvements or alternatives.

This paper began life as a commissioned scoping study to inform and advise PEIC about new and emerging developments in information and communication technology relevant to the collection, sorting, analysis, storage and dissemination of data about attacks on education. Once the study had been completed, however, it was apparent that no other up-to-date overview of the relevance of such developments to the

'attacks on education' agenda was publicly available. Consequently, Jane Kalista was requested to adapt her initial study for the benefit of a wider audience. PEIC is grateful to Ms Kalista for this informative, balanced and useful analysis of how 'humanitarian technology' may not only supplement and complement tried and tested approaches but may also generate new types of information about attacks on education.

Mark Richmond
Director, Protect Education in Insecurity and Conflict (PEIC)
Education Above All Foundation

GLOSSARY OF TERMS

Big data, or big data analytics: 'the range of tools and methodologies that use advanced computing techniques to leverage largely passively generated data, for example, those resulting from the use of mobile phones or social networks, and the active collection of observed data by satellites, for example, to gain insights for decision-making purposes' (Letouzé, Meier and Vinck, 2013, as cited in IFRC, 2013, 15).

Crisis mapping: '"leverages mobile and web-based applications, participatory maps and crowdsourced event data, aerial and satellite imagery, geospatial platforms, advanced visualization, live simulation, and computational and statistical models to power effective early warning for rapid response to complex humanitarian emergencies"' (Crisis Mappers, as cited in IFRC, 2013, 15).

Crowdsourcing: 'the process of "obtaining needed services, ideas, or content (e.g. data) by soliciting contributions from a large group of people, and especially from an online community, rather than from traditional employees or suppliers"' (Merriam-Webster, as cited in IFRC, 2013, 15).

Digital data collection: 'the process of replacing traditional assessments conducted with pens and papers by data collection by humanitarian actors and, where possible, affected populations, supported by widely available and usable digital devices such as smartphones. This results in substantial gains in terms of speed and quality of the data' (IFRC, 2013,15).

Information forensics: 'involves the process of verifying crowdsourced social media information or determining the credibility of social media reporting' (iRevolution.net).

Microtasking: 'the process of taking a large task and breaking it down into a series of smaller tasks and which, in the context of humanitarian technology, typically is used to refer to human computing that involves the processing of large amounts of information by digital volunteers, for example, the tagging and geo-location of disaster tweets or images' (iRevolution.net).

Remote sensing: 'collecting and interpreting information about the environment and the surface of the earth from a distance, primarily by sensing radiation that is naturally emitted or reflected by the earth's surface or from the atmosphere, or by sensing signals transmitted from a device and reflected back to it. Examples of remote-sensing methods include aerial photography, radar, and satellite imaging' (Esri GIS Dictionary, esri.com).

Sentiment analysis: '…the use of real-time, active listening through analysis of social and online media to ascertain trends in perceptions of a particular intervention or development' (iRevolution.net).

INTRODUCTION AND PURPOSE

Since the publication of the first *Education under Attack* study in 2007, the quantity of available data on attacks on education has increased considerably owing to a number of factors. A greater number and more diverse mix of local, national and international media are now accessible online. Awareness and interest among UN agencies, NGOs, human rights groups and media have grown, as reflected by the number of reports and case studies published that focus specifically on attacks on education. Coverage of attacks on schools by the UN Monitoring and Reporting Mechanism (MRM) on grave violations of children's rights in armed conflict has also increased. Similarly, Education Clusters at country level are increasingly collecting and publicising data about attacks in the contexts where they operate. The rapid rise of internet, mobile phone and social media use is producing ever increasing amounts of content or 'big data' to be mined. The net result is a large and growing volume of available information to be collected, sorted and used effectively for strengthening the protection of education in situations of conflict and insecurity.

As became apparent during the preparation of the most recent *Education under Attack* study published in February 2014, dealing with this expansion in available information requires significant investments of time and resources. Current trends suggest that the quantity of data to be marshalled will only continue to increase, creating challenges for reliably capturing and using information from a significant (and increasing) number of possible sources.

At the same time that data are becoming increasingly available, there are also still a number of gaps. For example, higher education lacks

formalized local or national monitoring structures, and, consequently, there is much less systematically collected data available regarding attacks on higher education facilities, students, academics and other personnel. Furthermore, both the UN MRM and the Education Cluster have become increasingly useful sources of data, but these mechanisms are not present in every country where a pattern of attacks may be occurring – and, in the case of the MRM, capture only those incidents that can be verified by the UN, which may be a small subset of the total number of attacks. Particularly insecure areas – which are often the most likely sites of attacks – may be most difficult for journalists and UN and NGO staff to reach or may discourage local civil society from reporting incidents for fear of retribution; coverage in such areas may be extremely limited or, at best, second- or third-hand. In countries where information is tightly controlled and where governments may themselves be the perpetrators of attacks, reliable data about attacks and means of verification are also likely to be quite limited.

The recent GCPEA report *Education under Attack 2014* calls for a range of stakeholders to improve the collection and use of information about attacks on education in order to hold perpetrators to account, devise effective prevention and response measures, and address the impact of such attacks. In seeking to strengthen the monitoring and reporting[1] of attacks on education, it may be useful to look to the growing field of humanitarian information and communication technology for possible tools to help address these challenges – in terms of both collating rapidly-increasing quantities of data and seeking to close data gaps.

This paper is intended to provide a preliminary look at a number of innovations in the field of humanitarian information and communication technology and their possible applications to the monitoring and reporting of attacks on education. It is meant to serve as a starting point for deeper reflection among partners involved in protecting education and for informing exploratory discussions with experts in technology and innovation. Based on a desk review of existing reports, practitioner blogs and websites, and conversations with relevant experts, consideration is given to the potential complementary uses of such technology for collecting, verifying and analysing data and for generating new opportunities for the collection of primary data. Advantages and risks are discussed and a number of conclusions and recommendations are presented.

It should be noted that the potential uses of humanitarian technology and innovation in field-based prevention and response programmes are also worth exploring in greater depth, in collaboration with relevant partners and in conjunction with efforts to improve both country-level interventions and global responses. Several programmes have used innovations in technology – such as mobile alerts to warn students, parents and teachers about dangers at or in the vicinity of schools[2] or

[1] For the purposes of this paper, 'monitoring and reporting' is used in its broader sense – namely, the systematic collection, analysis and use of data regarding attacks on education and their impacts by a range of actors. This encompasses but is not limited to UN Security Council mandated monitoring and reporting on grave violations of children's rights in armed conflict.

[2] See, for example: 'UNESCO Uses Souktel Mobile Alerts System to Keep Gaza Schools and Students Safe,' Souktel, 31 October 2011, http://www.souktel.org/media/news/unesco-uses-souktel-mobile-alerts-system-keep-gaza-schools-and-students-safe

use of social media for advocacy and awareness-raising – as part of an effort to keep students and teachers safe, and provide promising examples; others might be developed to support community protection of schools or the alternative delivery of learning, for instance. However, such potential uses are not addressed in the analysis that follows due to a deliberate focus on monitoring and reporting of incidents and impacts, and on linking humanitarian technology specifically to data needs regarding attacks on education.

WHAT IS 'HUMANITARIAN INFORMATION AND COMMUNICATION TECHNOLOGY'?

Rapid innovations in technology are changing the landscape of humanitarian action and opening new avenues for improving preparedness, response and recovery (IFRC, 2013; OCHA, 2013). 'Real-time' data acquisition, sorting, analysis and communication are increasingly recognized as integral to effective humanitarian response (Harvard Humanitarian Initiative Working Group on Applied Technology for Humanitarian Action, 2009; OCHA, 2013). With mobile phone and internet use on the rise around the world, advances in the growing field of humanitarian technology are facilitating such data collection and analysis (particularly as the quantity of data being generated – including by affected communities themselves – increases exponentially and is increasingly digital) (Independent Expert Advisory Group on a Data Revolution for Sustainable Development, 2014; IFRC, 2013; Mancini, ed., 2013; Meier, 2011; OCHA, 2013). While many of the recent uses of this technology have occurred in crisis responses to major natural disasters, there are also a number of promising examples of its use in the documentation of human rights abuses,[3] the reporting of child

[3] See, for example: Harvard Humanitarian Initiative, 'Satellite Sentinel Project', http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program; Amnesty International USA, http://www.amnestyusa.org/research/science-for-human-rights/remote-sensing-for-human-rights; Human Rights Watch, 'Sudan: Satellite Images Confirm Villages Destroyed,' 18 June 2013, http://www.hrw.org/news/2013/06/18/sudan-satellite-images-confirm-villages-destroyed, 'Burma: Satellite Images Detail Destruction in Meiktila,' 1 April 2013, http://www.hrw.org/news/2013/04/01/burma-satellite-images-detail-destruction-meiktila, and 'Syria: New Satellite Images Show Homs Shelling,' 2 March 2012, http://www.hrw.org/news/2012/03/02/syria-new-satellite-images-show-homs-shelling.

protection and gender-based violence issues,[4] and the analysis of patterns and trends of violence across space and time.[5]

Humanitarian information and communication technologies include new tools for humanitarian action such as big data analytics, crowdsourcing, crisis mapping, digital data collection, microtasking, remote sensing, sentiment analysis and information forensics (IFRC, 2013; iRevolution.net). These tools have the potential 'to detect needs earlier and predict crises better, enable greater scale, speed and efficiency of response and assistance delivery, enhance the specificity of resource transfers to match needs of communities at risk, and increase accountability and transparency' (IFRC, 2013, 14).

Developments in advanced computing (i.e. human computing and machine computing) are making it more and more possible to sort through, make sense of, visualize and even begin to verify Big (Crisis) Data as well as Big (Development) Data (iRevolution.net). Human computing uses crowdsourcing and microtasking platforms to allocate data management tasks to a 'crowd' of humans, while machine computing uses machine learning and automated data mining to manage more difficult tasks or ones that are nearly impossible for humans to complete (IFRC, 2013). Both aspects of advanced computing are currently being used and further developed to manage the big data challenge in humanitarian crises and the related issue of verifying user-generated content (IFRC, 2013; iRevolution.net).

Digital tools are also enabling improved primary data collection and management – increasing speed, quality and ease of analysis – and opening two-way channels of communication between affected communities and humanitarian agencies (IFRC, 2013; ICRC, 2013; OCHA, 2013; Meier, 2011; Meier and Leaning, 2009). Not only do such tools enable humanitarian agencies to obtain data more efficiently and to share and amplify the dissemination of vital information for crisis prevention and response, but they also allow affected individuals and communities to demand greater accountability and transparency, as well as to communicate useful feedback regarding needs and perceptions for better informing humanitarian efforts (IFRC, 2013). In addition, communication technologies are improving the prevention, preparedness and response efforts of communities themselves – most often the first responders to a crisis – facilitating their self-organization, enabling local responses and contributing to resilience (IFRC, 2013).

The table below, taken from the IFRC's *World Disasters Report 2013*, provides a useful overview of types of technological innovations that

[4] See, for example: *Mobile Technologies for Child Protection: A Briefing* Note, UNICEF 2011, http://www.unicef.org/cbsc/files/mobile_technologies_for_child_protection.pdf; New Tactics in Human Rights, 'Empowering communities with technology tools to protect children,' October 2012, https://www.newtactics.org/conversation/empowering-communities-technology-tools-protect-children; STATT, *Tackling Gender-based Violence with Technology: Case Studies of Mobile and Internet Technology Interventions in Developing Contexts*, 2014, http://hirondelleusa.org/wp-content/uploads/2014/09/STATT-Tackling-GBV-with-Technology.pdf; Ayiti SMS SOS, http://survivorsconnect.org/haitismshelpline/main

[5] See, for example: Dr Colleen McCue, 'Pattern analysis of the LRA and IDPs', http://www.youtube.com/watch?v=4idbNE-xUoA and Dr Jen Ziemke, 'CrisisMappers Webinar Series - Advanced Visualization & Analysis applied to Conflict Mapping,' http://www.youtube.com/watch?feature=player_embedded&v=dfSJflcxPGo

have already been, or are nearly ready to be, implemented during different phases of humanitarian action:

Table 1.1 Examples of technological innovations for use in humanitarian actions

HUMANITARIAN ACTION PHASES	SELECTED ACTION	SELECTED TECHNOLOGICAL INNOVATIONS
Mitigation	Early warning	Big data analytics for early warning, including social media, satellite imagery, etc.
		Advances in computing
		Text messages and social media warning systems
		Open data, access through social media
Preparedness	Planning and training	Resource databases and social networks
		Online distance learning platforms and discussion platforms, mail lists
		Mobile platforms
		Social media campaigns
Response and recovery	Situational awareness and needs analysis	Big data analytics
		Information sharing platform
		Mobile and digital data collection
		Satellite imagery, aerial photography, unmanned aerial vehicles
		Crowdsourcing information
		Micro-tasking
		Secure data transmission and encryption
		Long range data transmission
	Resource management and accountabillity	Resource mobilization through social media
		Mobile cash transfers
		Commodity and resource tracking through mobile phones
		SMS-based feedback from affected people receiving aid

	Resource management platforms
	Matching needs and volunteers through social media
Search and rescue	Reunification through social media
	Search and identification through 'digital signature' (e.g., mobile phone SIM card)

Source: IFRC 2013, 21.

Humanitarian technology is gaining considerable ground in terms of interest and the development of tools and communities of practice – and its use is an inevitable part of a natural evolution in humanitarian action (IFRC, 2013). However, systematic and rigorous evaluations are still lacking, and there remain essential ethical and practical questions that warrant careful consideration (IFRC, 2013; OCHA, 2013). For example, disparities in access to technology may introduce harmful bias or exclude particular individuals or groups; two-way communication may raise expectations among individuals and communities that are subsequently not met by organizations collecting information; dependency on technology may introduce vulnerabilities when such technology fails; crowdsourced data may be used for nefarious purposes or manipulated by governments, armed groups, or their supporters or opponents; lack of exposure to or experience with modern information technology may make it difficult for people to give genuine informed consent; and the risk of information misuse and compromised data security and privacy can be a real issue, both short- and long-term (ICRC, 2013; IFRC, 2013; OCHA, 2013). Security risks incurred by users and collectors or contributors of information are also a critical issue, particularly in situations of conflict or under repressive regimes (ICRC, 2013; IFRC, 2013; OCHA, 2013).

A number of steps have been taken to address issues of security and to establish ethical standards and guidelines for the use of humanitarian technology to ensure that it adheres to the fundamental humanitarian 'Do no harm' principle.[6] The ICRC recently revised its *Professional Standards for Protection Work* handbook, including a discussion of the use of new technologies in its guidance for the management of sensitive information, for example (ICRC, 2013). However, it is clear that each case warrants a thorough examination of potential risks and that the decision to use different technologies for systematic data collection on sensitive issues must be based on careful analysis of such risks, weighed against benefits and compared with other means, and on the ability to ensure appropriate safeguards without compromising humanitarian principles (ICRC, 2013; IFRC, 2013; Mancini, ed., 2013).

[6] See, for example, the development of a code of conduct by the Standby Task Force: http://blog.standbytaskforce.com/2012/02/14/data-protection-standards-2-0/ and GSMA Disaster Response, Souktel and the Qatar Foundation, *Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters:* http://www.souktel.org/sites/default/files/resources-files/Towards-a-Code-of-Conduct-SMS-Guidelines.pdf

HOW CAN HUMANITARIAN INFORMATION AND COMMUNICATION TECHNOLOGY CONTRIBUTE TO MONITORING AND REPORTING OF ATTACKS ON EDUCATION?

Humanitarian information and communication technologies have the potential to strengthen the collection, analysis and use of data regarding attacks on education, including by facilitating the work of UN and NGO partners on the ground as well as the sharing of that information at global level. Not only might they support data gathering, analysis and use for rapid response and accountability, but they also stand to help in warning of trends of attacks in particular areas, in contributing to prevention and early warning, and in analysing patterns over time and across locations.

The following section discusses possible applications of these technologies to monitoring and reporting both of individual attacks on education and their effects in ways that stand to complement existing methods of gathering and analysing incident and impact data. Some of the innovations mentioned below may already be in use or in the process of being explored, in which case there may be opportunities for partnerships, knowledge-sharing and capacity-building to improve and expand the use of existing tools and the development of new ones.

Potential risks and/or costs associated with these types of data collection, however, may be acute and therefore warrant careful consideration. The options outlined below would need to be examined with due caution, including in terms of risks and resource implications as weighed against benefits, and developed further in consultation with

relevant technical experts. However, they do give an idea of avenues that might be explored in further depth.

Digital data collection

Opportunities: One of the most straightforward applications of technology is the use of mobile devices for the collection of data. A number of platforms have been developed that enable researchers to collect data using mobile devices, whether smart phones and tablets or basic mobile phones – for example, in conducting humanitarian assessments,[7] health surveys, or monitoring and evaluation of programmes – and send it instantaneously to a central repository where it is cleaned, stored and made ready to be analysed. Such tools could be used for recording incidents of attack and assessing their impacts when surveying affected communities. Mobile phones can also be used to send surveys directly to communities, soliciting their feedback on a given question or set of questions via free SMS. This could be useful, for example, in collecting impact data or data about community responses to attacks.

If approached collaboratively and with agreed indicators and processes across countries, these tools could support the standardization of collection and coding of data on attacks on education for use by accountability mechanisms (such as the UN MRM), as well as by field-level stakeholders. Both standard terms and consistent collection of incident and impact data would also help to strengthen global advocacy and research.

Challenges: The security of data collectors and contributors as well as of the data are the foremost concerns. Technology failures and loss of data are also possible risks. Most technologies include strong security features, including full device encryption for smartphones.[8] Data are typically encrypted when collected and submitted using smart devices and backed up regularly on central servers; however, data sent via SMS from mobile phones cannot be protected. Internet access constraints are unlikely to present a problem, as data can be stored in a tablet or smartphone and transmitted at a later point in time, once online. However, data that have not yet been sent to the server can be lost in the meantime if anything should happen to the device on which they have been collected.

With respect to survey distribution and responses, ensuring privacy and protection of data would need to be a pre-condition and the potential sensitivities and contextual risks to participants would need to be assessed before pursuing this option further. There may be fewer risks to using digital means to replace paper data collection by individual

[7] The Education Cluster, for example, has used digital data collection tools for conducting education needs assessments in emergencies, which include capturing information about attacks and their impacts where relevant.
For more information, please see http://educationcluster.net/what-we-do/knowledge-management/
and http://educationcluster.net/topics-lp/information-and-knowledge-management/.

[8] See, for example, Magpi: http://home.magpi.com/ or Souktel: http://www.souktel.org/dev-products/polling-data-collection. Medic Mobile, http://medicmobile.org/platform, is another digital data collection platform for healthcare workers which is designed to be used in hard-to-reach areas with little or no access to internet and limited access to electricity.

researchers or field staff conducting assessments or other surveys; however, the idea of surveying individuals via SMS or of creating a free SMS short code whereby individuals could send information regarding attacks and impacts is potentially more problematic from a security perspective, depending on the likelihood and/or capacity that governments or armed groups might be able to intercept or trace such communications.

While data can be encrypted on smart phones and tablets, this requires that users take the necessary steps to do so but even then it is not fool-proof; in addition, more basic mobile phones have no way of encrypting or securing content and network providers have access to all data. There is also the question of obtaining informed consent from users who might not be fully aware of the potential consequences of participating or of sharing information. The context therefore needs to be considered very carefully before using this method of data collection. Another option, depending on the context, might be to use broadcast messaging via mobile (e.g. SMS or voice messaging) with information about where and how to report attacks and their impacts.

Crisis mapping

Opportunities: Crisis mapping offers a potential set of tools to develop maps that highlight hotspots and can link traditional media and social media reports, as well as information received via SMS or internet, to locations in near real-time on an interactive map. These maps can either be publicly shared and open to input from the 'crowd' or can be secured for private use within an organization or among a particular set of users. Even if open to 'crowd' input, reports can be reviewed and verified by an administrator before being posted to the map.

Data on attacks and their immediate impacts could be collected and/or visualized in this way, either at the level of individual countries or at global level. Developing crisis maps would enable geolocation of incidents and would highlight affected areas in ways that could potentially be useful for responders as well as for advocacy purposes. There are a number of ways this could be done, ranging from content entered exclusively by UN Country Task Forces on Monitoring and Reporting (CTFMRs) or Education Clusters, for example, or an agreed set of users at country, regional or global level, to inclusion of incidents reported by individuals once verified against other reports (which would also open a new avenue for primary data collection).[9]

Ushahidi's 'Crowdmap' (http://www.ushahidi.com/product/crowdmap/) is one open-source platform that could be of interest and has been used

[9] Some interesting examples of relevant crisis mapping project examples include: Voices of Kibera, which is a component of the project 'Map Kibera', a citizen mapping and reporting/interactive community information project in the Kibera area of Nairobi, Kenya: http://voiceofkibera.org/main; Ayiti SMS SOS Human Rights Observatory & Helpline Initiative, a mapping platform set up in Haiti after the earthquake to track reports of violence and human trafficking: http://survivorsconnect.org/haitismshelpline/main; and SyriaTracker, which uses a combination of crowdsourcing tools to capture information from citizen journalists and data mining tools to scan online media and social media reports: http://www.humanitariantracker.org/#!syria-tracker/cj00.

by a number of UN agencies and NGOs,[10] and there may be others. Such a platform could be customized to create a detailed map that visualizes the location of incidents and links them to their sources, whether for public use or for sharing exclusively with a closed group of users. Ideally, efforts could be undertaken to map the locations of all existing schools (formal and non-formal) and higher education institutions, if such a map does not already exist in a given context, using basic GPS devices, and this could serve as the map used for visualizing the location of incidents if and when they occur. Alternatively, a basic digital map of a country or locality could be used where security, resource or other constraints prevent mapping the locations of all education facilities (as opposed to only those affected by attacks). Eventually, other types of incidents, needs or services could be plotted onto the same map, enabling users to see where different types of problems cluster and where stakeholders should prioritize concerted interventions.

Challenges: The range of risks depends largely on whether or not such mapping would be available to the public and the extent to which crowdsourcing of incident information is used. Even if purely a map of incidents reported in online media and public UN and NGO reports, one of the main concerns is that making this visual information publicly available could in some way draw negative attention and do unintended harm if picked up and used by the wrong hands. For example, geolocating a report of a school being used by armed forces or highlighting an area in which a number of schools are reported to be used by military forces could exacerbate their vulnerability as targets. The specificity of such a map may mean it is better designed for restricted access to relevant partner organizations and for use as a rapid response tool, rather than for public reporting.

If open to information from the 'crowd', protocols for verification would need to be put in place; and while some degree of verification of social media sources is increasingly made possible by new technologies, it may still be possible for false or manipulated information to slip through. There are also questions regarding the security of users who might be submitting content, particularly in contexts where governments may be more sophisticated in their surveillance of ICTs; security measures such as data encryption may help to mitigate in some contexts but a considerable degree of risk remains.

Crowdsourcing and 'crowdseeding' data collection

Opportunities: Crowdsourcing data collection is another potential and growing means of obtaining primary data. The underlying principle is that data are obtained via contributions from a 'crowd' or wider community through an open call for information. This may include using open crisis maps, as discussed above, via which users can submit reports, videos and images of incidents of attacks on education or military use of education facilities and/or impacts of such incidents; collection, vetting and sorting of relevant social media data; the development and use

[10] Both the USIP 'Special Report' *Crowdsourcing Crisis Information in Disaster-Affected Haiti,* 2010, http://www.usip.org/publications/crowdsourcing-crisis-information-in-disaster-affected-haiti and the UNICEF WCARO publication *Mobile Technologies for Child Protection: A Briefing* Note, UNICEF 2011, http://www.unicef.org/cbsc/files/mobile_technologies_for_child_protection.pdf, provide useful information and insights regarding use of Ushahidi by UN agencies and NGOs.

of mobile applications that enable individuals to share images and/or reports;[11] or the creation of a free short code number or hotline to which users could text or call in reports of incidents or impacts as they are observed. A number of tools are being developed to increase the reliability of crowdsourced data, including a platform for crowdsourcing the verification of such data and a smart phone application that enables citizen journalists to upload images and/or video content from internet-enabled media devices that meets requirements for use in legal prosecutions.[12]

A slightly more restricted or controlled form of crowdsourcing has been referred to as 'bounded crowdsourcing' and is similar to 'snowball sampling' in statistics (iRevolution.net; IFRC, 2013). Bounded crowdsourcing begins with the selection of a small number of trusted individuals, who in turn are asked to select a designated number of reliable individuals for whom they can vouch to join the data collection effort (iRevolution.net). The boundary remains dynamic and therefore can increase the number of contributors while maintaining a greater degree of reliability than open crowdsourcing (iRevolution.net). However, reports are accepted only from approved participants (USIP, 2010).

A third and even more restricted form of crowdsourcing, referred to as 'crowdseeding', might also be considered and may have an even higher degree of reliability in terms of data quality. Crowdseeding involves identifying a limited number of reliable sources within a given number of randomly selected communities and giving them a means of reporting information, whether via mobile phone or otherwise (IFRC, 2013).

This method was utilized by Columbia University in South Kivu in the Democratic Republic of the Congo (DRC) in a project called 'Voix des Kivus', which sought to use mobile phone technology to gather verifiable, high-quality data about conflict events in real time (van der Windt and Humphreys, 2012; Voix des Kivus project summary, 2011), and provides an illustrative example. A random sample of eighteen villages was selected and specific reporters from three groups were identified (i.e. one representing the traditional leadership, one representing women's groups and one elected by the wider community) in each village. They were given mobile phones, credit, training and a code sheet for reporting incidents of violence. According to IFRC (2013), this system had three benefits in terms of data quality: 1) people could participate who otherwise would have been unlikely to do so, given that many lived in remote villages and lacked mobile phones or the money

[11] See, for example, UNICEF's mobile application 'U Report', a free application for youth which enables 'U-reporters…[to] connect through a range of communication channels to voice their opinions about what is happening in their communities and work together with leaders at the community and national level for positive social change': http://www.ureport.in/

[12] See, for example, the International Bar Association's (IBA) 'eyeWitness to Atrocities' project, currently being rolled out, which, according to the IBA project description (2014), 'capitalizes on the ubiquity of mobile devices, and the increasing use of social media to report atrocities, by providing a tool to document international crimes in a secure and verifiable way. This cutting edge technology captures videos in a manner that will facilitate their use as evidence in a court of law. This project will magnify the impact of the videos collected every day by citizen journalists and human rights defenders around the world.' For more information, see http://www.newperimeter.org/our-work/access-to-justice/eyeWitness.html and https://guardianproject.info/informa/.

to send SMSs; 2) using random sampling ensured that the information was representative of a wider population; and 3) the possibility of faking reports was limited, particularly as the system enabled relationship-building with the reporters, increased incentives to report truthfully, and made it possible to cross-validate reports. Participation was free and fully consensual. Data were received by software that automatically filtered the messages, coded them for content, cleaned them to remove duplication and merged them into a database (van der Windt and Humphreys, 2012; IFRC, 2013).

According to the project's researchers (van der Windt and Humphreys, 2012), 'The data that was generated was rich; including regular reports of conflict events: encroachments by various groups, abductions, looting, shootings, and sexual violence. Messages also contained accounts of crop failures and floodings, as well as of interventions by development organizations and other actors. Beyond reporting, the system was used in some cases simply to make requests, for support with a health clinic, for support with schooling.' Because the system made use of identifiable users (in contrast to the anonymity of crowdsourcing), the project kept sensitive event data confidential and shared such data only with approved organizations in a position to respond; data were communicated using numbers that corresponded to particular types of incident rather than text; participating villages remained mutually anonymous for security reasons; and the scale of the project was kept small to avoid drawing attention – including from violent groups, among others – and endangering reporters (IFRC, 2013; van der Windt and Humphreys, 2012). (Please see IFRC, 2013, 48-49 for a summary of the project and van der Windt and Humphreys, 2012 for a more detailed discussion of the project components and lessons learned.)

Challenges: Crowdsourcing primary data collection comes with a number of potential challenges. The difficulty of verifying data and the potential for manipulation or misrepresentation of information are considerable, calling into question its reliability – although it has been argued that use of crowdsourcing can be self-correcting. It may be more appropriate to consider using information provided through crowdsourcing as an alert to look more deeply into a reported incident. There are also security risks to providers of data – particularly for means of communication that cannot be encrypted or otherwise protected – which need to be measured on a case-by-case basis. Furthermore, providing a free short code for users to send reports via SMS may raise expectations of concrete and timely responses that, if unmet, could disillusion users, discourage use of the reporting system and potentially damage the credibility of organizations working on the ground.

Crowdseeding appears to better control for the quality of data; however, there are important risks for reporters. While SMSs may use numerical code rather than words for security reasons, if intercepted, this could actually cause more harm to reporters, who might be suspected of suspicious activity. In the example from DRC cited above, there were no recorded cases of humanitarian organizations acting on or responding to the information that was obtained from reporters and shared with them on a regular basis (van der Windt and Humphreys, 2012; IFRC, 2013) – posing an ethical question for the collection of such data and the benefits to the communities reporting.

Remote sensing

Opportunities: Remote sensing – including satellite and aerial imagery – has been used in a number of conflict situations to monitor and document human rights violations, including the destruction of civilian infrastructure and forced displacement. Amnesty International USA, Human Rights Watch, the Harvard Humanitarian Initiative and others have used satellite images to be able to count targets or monitor the human security of civilians over time in situations of armed conflict – see, for example, Harvard Humanitarian Initiative's 'Signal Program on Human Security and Technology', which is building on lessons learned from the pilot phase of its Satellite Sentinel Project in Sudan from 2010 to 2012 (http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program).

An example of particular relevance to the issue of attacks on education is a project recently undertaken by the Geospatial Technologies and Human Rights Project of the Association for the Advancement of Science (AAAS) at the request of Physicians for Human Rights (PHR). AAAS analysed high-resolution satellite imagery to examine medical facilities in several cities across Syria and verify reports of damage and destruction collected via traditional news media, social media and PHR's network of contacts on the ground. By using satellite imagery, verification could be performed remotely and reliably for a context in which it would have been difficult to verify both the location and dates of damage reports due to high levels of violence and insecurity across the country (for more information, see http://www.aaas.org/page/assessing-status-medical-facilities-syria).

While the cost of obtaining satellite imagery can be high, a number of companies – for example, DigitalGlobe – are able to provide discounted or free services for social sector projects. There are also a number of lower cost providers coming onto the market. Collaboration with partners already working in this area – for example, human rights organizations – might be pursued so as to test the utility of remote sensing for gathering or verifying attacks data in a selected number of countries.

Other forms of remote sensing are also emerging and may gain ground as technology continues to develop. For example, the UN Security Council approved the trial use of unmanned aerial vehicles (UAVs), or drones, by the UN peacekeeping mission to monitor the movement of militia and armed groups in eastern DRC,[13] and there have been discussions about adding similar capacity in other UN missions (OCHA, 2014). It is possible that UAVs could eventually be used to gather aerial imagery from hard-to-reach locations to verify attacks and resulting damage, but at present, their use for humanitarian purposes in conflict zones remains highly controversial, particularly given the military use of drones in a number of contexts and concerns over privacy, ownership and use of data (OCHA, 2014; iRevolution.net).[14]

[13] See http://www.unmultimedia.org/tv/unifeed/2013/12/drc-drones-launch/

[14] For a more detailed discussion of these issues, please see OCHA's Occasional Policy Paper 'Unmanned Aerial Vehicles in Humanitarian Response', June 2014: https://irevolution.files.wordpress.com/2014/07/unmanned-aerial-vehicles-in-humanitarian-response-ocha-july-2014.pdf. See also 'Reflections on the Use of UAVs in Humanitarian Interventions,' 6 September 2014, http://irevolution.net/2014/09/06/reflections-on-uavs-in-humanitarian-interventions/

Challenges: Use of satellite imagery is likely to be most relevant for monitoring and verification of attacks on education infrastructure and some instances of military use – particularly in insecure or hard-to-reach areas or under repressive regimes where information and movement are limited. Although it may be a useful tool for verifying reports in areas that are impossible to reach for security and other reasons or for flagging up potential incidents or cases of military use, this tool requires additional knowledge to confirm both the cause of the damage and the questions of intent and likely perpetrator. It should be seen as a complement, therefore, rather than a primary data collection tool in and of itself.

There are also some types of damage it will be unable to verify – for example, to sides of buildings that cannot be seen from an aerial view. In addition to the possible costs associated, there are additionally the issues of resolution quality, weather and geography. To be able to get the level of detail needed to verify damage to or military use of a school, high-resolution images are needed; many of the more readily available satellite images are likely to be too low-resolution to be useful for such purposes. Also, cloud cover or other weather patterns or the heavy presence of vegetation can make it difficult to obtain useful images.

Geospatial analysis to understand patterns and trends

Opportunities: A number of geographic information system (GIS) platforms exist that enable the visualization, analysis and interpretation of data to better understand patterns, trends and relationships. These platforms can be connected directly with a database and can be used securely. They would enable the mapping and visualization of data and the detection of hot spots and trends that could be followed over time, including through the visualization of space-time or time series data in ways that may make it easier to see historical patterns. Several such platforms also have the capability to use modelling for prediction that could be of potential use for strengthening prevention, preparedness and early warning. Drawing from the field of predictive analytics (used most often in the commercial sector but also in law enforcement), geospatial predictive analysis could also be undertaken, using a combination of spatial event data, human geography and physical geography to build supervised learning algorithms for modelling and pattern analysis that can be used for prevention, early warning, mitigation and response.[15]

Challenges: The cost of obtaining access to these technologies would have to be weighed against the potential benefits of their use. The visualization of data enabling analysis of historical patterns and trends is likely to be of interest and use to researchers as well as to actors engaged in advocacy. However, it is also important to consider how to ensure that such visualization of data be made useful and timely on the ground for strengthening prevention and anticipating response needs – particularly with respect to predictive analytics.

While predictive modelling may be useful in designing prevention and preparedness measures, such modelling will inevitably contain inaccuracies and may also be hindered by incomplete information

[15] An interesting example looks at a range of attacks by the Lord's Resistance Army (LRA) and movements of internally displaced persons (IDPs) across the border regions of Central African Republic, DRC and South Sudan – please see the work of Dr Colleen McCue on 'Pattern analysis of the LRA and IDPs': http://www.youtube.com/watch?v=4idbNE-xUoA.

about perpetrators and motives. It may offer a useful indication in many cases where there are existing patterns of attack, but predicting rare events, for example, may be much more difficult (Letouzé, Meier and Vinck in Mancini, ed., 2013).

Monitoring social media

Opportunities: Social media (including Twitter, Facebook, Instagram and Flickr) have yet to be used in the monitoring of attacks, but they are a fast-growing potential (though controversial) source of information, at the very least, as a trigger to look into a reported incident using other sources and contacts on the ground. As humanitarian technology continues to develop, methods for verifying or assessing the credibility of user-generated content are improving. While there is a risk that such media might be used to spread rumours or propagate mass misinformation, it has been argued that these tools are often self-correcting (iRevolution.net). New methods for detecting whether videos have been altered and for ensuring that they provide key information such as the date, time, geographic coordinates and the identity of subjects and have a trusted chain of custody are emerging,[16] increasing the potential for citizen journalism to be used in the documentation and even prosecution of human rights abuses. Information communicated via these media can also increasingly be triangulated – for example, if social media reports of a particular incident begin to cluster in a location with limited access for journalists and humanitarian workers, satellite imagery might be used to verify an attack on infrastructure or a case of military use. Furthermore, taking the pulse of social media on the issue of attacks on education could be useful for advocacy purposes, as well as for improving field-level responses.

Since social media remain largely unexplored territory for research on attacks on education, it is difficult to know the extent to which incidents are being reported first-hand via social media platforms. It is likely that the number is limited in many of the places where attacks are occurring, in part because of limited or restricted coverage of or access to technology. However, for events occurring in contexts where access to technology enables social media use, such as Syria, the picture may be very different. There are also likely to be broadcasts of information reported by UN or media sources, and considerable second-hand social media activity around high profile events.

A number of tools and resources could be used to get a better picture of what might exist in the way of relevant social media. A platform like Geofeedia (http://geofeedia.com/how-it-works), which enables searches of social media entries by location rather than hashtag or keyword, might be used in a number of sample contexts to review social media use in areas where attacks are known to occur or where a documented attack has just taken place to see whether and how much incidents are being reported via social media. The Qatari Computing Research Institute's Artificial Intelligence for Disaster Response (AIDR) platform and/or Ushahidi's 'crisisNet' (http://www.ushahidi.com/product/crisisnet/) might also be used to monitor and mine social media and classify results according to specific criteria.

[16] See, for example, eyeWitness to Atrocities Project: http://www.newperimeter.org/our-work/access-to-justice/eyeWitness.html and https://guardianproject.info/informa/

Challenges: Considerations include the degree of accuracy of incoming data, the utility of monitoring social media relative to the effort and resources required, and the reliability of such information as a source. As mentioned above, information obtained via social media is highly variable in quality and can be easily manipulated or reflect clear bias, posing challenges for verification and validity. Although argued to be self-correcting, the possibility of organized misinformation is also considerable, enabling rumours to propagate quickly. It is not known how many attacks on education or impacts of such attacks might actually be reported in this way, particularly by those communities affected; the number is presumed to be limited, given many of the contexts in which attacks occur and questions of access to technology that enable social media use (although such access is only likely to increase over time). As sources unto themselves, therefore, social media reports may be problematic, and are likely better used for purposes of triangulating information or as leads for further investigation of incidents or impacts.

Automating the search for and categorization of incidents reported in online media

Opportunities: One of the most time-consuming and resource-intensive aspects of the process of ongoing secondary data collection and analysis is the initial step of searching by key words for the range of different attacks for each affected, or potentially affected, country. Google searches, even when sorted by date or relevance, bring up hundreds of pages, many of which actually have no relevance at all. It may therefore be worth exploring whether at least some of this data mining could be automated, using machine learning to refine the computer's accuracy in pulling out relevant articles and reports. Several data mining tools exist, including a platform that is able to pull out relevant reports from a range of media sources using an established set of indicators (see, for example, the GDELT Project: http://gdeltproject.org/about.html#intro). It would be worth exploring whether such a platform could be used with a customized index of relevant search terms to capture information regarding attacks on education. It might also be possible to use algorithms to classify the information found in ongoing automated searches.

Challenges: While the appeal of being able to automate or semi-automate at least the initial phases of trawling online media reporting of attacks on education and their impacts is strong, there are a number of outstanding questions with respect to precision and efficacy. It remains to be seen whether automation could be sufficiently honed to minimize the inclusion of unrelated events or to categorize accurately. One of the principal risks is that information that a trained researcher might pick up could be lost. This step of the research also often involves a number of critical and complex judgment calls related to definitional fit, source and categorization that determine whether or not to include a particular incident or article and how to sort it.

It is conceivable that some of these types of judgements could be learned by a computer, or that automation could at least serve to collect large amounts of raw data that researchers could then review. However, there is a risk – as with any type of data collection – that some information could be missed or miscategorised, or that the costs of putting such a system in place may not outweigh the benefits if significant human resources are still required to sift through considerable 'noise'.

CONSIDERATIONS AND RISKS

A number of overarching considerations and risks can be distilled from the discussion of challenges with respect to each of the possible applications of technology outlined above. Foremost among these are security and ethical concerns.

Whereas a number of the technologies discussed above have evolved for purposes which are primarily apolitical (e.g. collection and monitoring of health data, natural disaster responses), both the nature of data on attacks on education and the politically-charged contexts in which such attacks typically occur are much more sensitive. Creating means by which individuals and communities can become more involved in monitoring and reporting may be beneficial but it may also put data collectors and contributors at considerable risk in some cases. Careful risk analysis needs to be undertaken on a case-by-case basis before any use of technology for data collection or dissemination is pursued and measures to mitigate possible risks should be an essential component of any initiative. Obtaining informed consent which makes clear the possible risks to providers of data needs also to be prioritized, and adherence to the ICRC's *Professional Standards for Protection Work* (2013) should underpin any application of new technologies for data collection and use.

Furthermore, actively soliciting information from individual reporters is likely to raise expectations that such data will generate concrete responses (e.g., repairs to damaged schools, alternative delivery of learning). Failure to follow up on data reported may jeopardise the goodwill and support of the individuals or communities providing it. Measures would therefore need to be put in place to ensure collectors

of such data (e.g. UN agencies, NGOs, governments) are accountable to its contributors, and to guarantee that reported information be followed up on and used to inform responses.

There are also a number of practical considerations to be weighed. Certain types of technology are likely to have substantial financial or human resource implications, or may simply not be feasible in some contexts because of variable access, availability and/or quality of technological infrastructure. Use of technology may increase the quantity of data that is able to be obtained, but means of sorting, verifying, securely storing and using such data need to be factored into time and resource allocations. The reliability and sourcing of data collected are also important issues, and require that appropriate quality controls be put in place.

While information and communication technologies are rapidly evolving and can be valuable tools for collecting, analysing and disseminating information, it is important that pursuing technological innovations not be undertaken for the sake of being at the cutting edge. Rather, the decision to use a particular type of technology in supporting data needs should be based on clear and demonstrated added value relative to the investments required and the risks incurred. A thorough consideration of benefits versus costs should be an essential first step, and possible uses should be piloted incrementally and evaluated rigorously before any major investment is made in a particular use of humanitarian information and communication technologies.

THE NEED FOR MULTIDISCIPLINARY PARTNERSHIPS

The research undertaken for this paper has highlighted the importance of multidisciplinary partnerships to maximize the potential contributions of technology and innovation to humanitarian action. Building partnerships among NGOs, research institutions and private sector companies working on the technology side, and UN agencies, human rights organizations, NGOs and researchers who have an interest in improving the monitoring and reporting of attacks on education will be critical to the success of any effort to adapt and use humanitarian information and communication technology to address data needs.

Learning from the experiences of those who have used some of these types of innovations in similar work – namely, the monitoring of human rights abuses and of child protection issues or other types of violence – should also be an integral part of any effort to use humanitarian information and communication technology to support monitoring and reporting of attacks on education and their impacts (whether primary or secondary data collection and/or analysis). Such experiences are likely to lend valuable lessons and insights, particularly related to the sensitive nature of data, risks incurred by data providers, use of social media data, and mechanisms for follow-up. (Please see Annex I for a list of potentially relevant organizations.)

CONCLUSIONS AND RECOMMENDATIONS

This briefing paper has outlined a number of potential uses of technology for the purposes of informing initial thinking about this area of work; there are undoubtedly others that may emerge should more in-depth collaboration be explored between stakeholders engaged in protecting education and relevant technology experts and/or as the field of humanitarian technology evolves. Each of these potential uses requires careful consideration of the security and ethical dimensions and a weighing-up of the potential risks against benefits. While more and better information can be an end in itself, specific attention needs to be given to what will be done with the information and how it might be more useful to partners than what might already be available. In-depth risk and cost-benefit analyses should be undertaken before any programming decisions are made, and the approach adopted should be a gradual and flexible one to ensure efficient and effective use of resources. Engaging key partners in the early stages of discussion will also be critical for ensuring that any investments made are realistic, seen to be useful and have the buy-in of these partners both as participants in and end-users of the process.

Engaging with the field of humanitarian technology and innovation holds much potential to develop tools and means for supporting improved monitoring and reporting and for responding to data needs about attacks on education and their impacts. More in-depth exploration and reflection are recommended, but many of these tools appear to have the possibility to increase the range of data able to be collected. They also stand to enable better analysis, visualization and sharing of data in ways that can strengthen responses and contribute to prevention and early warning. Despite the challenges posed, the adaptation and

use of humanitarian technology opens new opportunities to better protect education; and the salience of such use is only likely to grow as innovations continue to emerge and as access to different forms of technology continues to expand.

REFERENCES

Al Achkar, Z., Baker, I.L. and Card, B.L. (2013). 'Sharing Space: Adapting Military Approaches to Geospatial Analysis for Humanitarian Response and the Documentation of Human Rights Abuses,' Harvard School of Public Health – Program on Humanitarian Policy and Conflict Research Policy Brief, June 2013.

Bergtora Sandvik, K., Wilson, C. and Karlsrud, J. (2014). 'A Humanitarian Technology Policy Agenda for 2016,' Advanced Training Program on Humanitarian Action (ATHA) blog, 30 June 2014, http://www.atha.se/content/humanitarian-technology-policy-agenda-2016

Brookings, Google.org, Stanford Center on Democracy, Development and the Rule of Law (2012). 'New Technologies and Human Rights Monitoring, August 6-7, 2012 – Workshop Summary,' August 2012.

Drake, J. and Ashcroft, E. (2013). 'Eyes in the Sky: Remote Sensing in the Service of Human Rights,' *PhysicsToday*, February 2013, http://scitation.aip.org/content/aip/magazine/physicstoday/news/10.1063/PT.4.0072

Geber, T. (2014). 'Understanding Evidence: How Tech Is Complicating Law for the Better,' *TechPresident*, 28 May 2014, http://techpresident.com/news/wegov/25080/understanding-evidence-how-tech-complicating-law-better

GSMA Disaster Response, Souktel and the Qatar Foundation. *Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters*. London: GSMA.

Harvard Humanitarian Initiative (2009). 'Working Group on Applied Technology for Humanitarian Action,' http://hhi.harvard.edu/applied-technology-for-humanitarian-action

Harvard Humanitarian Initiative (2011). *Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies.* Washington, D.C. and Berkshire, UK: UN Foundation & Vodafone Foundation Technology Partnership.

Hayes, C. (2014). *Tackling Gender-based Violence with Technology: Case Studies of Mobile and Internet Technology Interventions in Developing Contexts*. Hong Kong: STATT.

Heinzelman, J. and Meier, P. (2013). 'Crowdsourcing for Human Rights Monitoring: Challenges and Opportunities for Information Collection and Verification' in *Human Rights and Information Communication Technologies: Trends and Consequences of Use*. IGI Global.

Heinzelman, J. and Waters, C. (2010). *Crowdsourcing Crisis Information in Disaster-Affected Haiti.* Washington D.C.: United States Institute for Peace (USIP).

International Bar Association (2014). 'eyeWitness to Atrocities: A Project of the International Bar Association (IBA)' – Project Description. London: IBA.

International Committee of the Red Cross (ICRC) (2013). *Professional Standards for Protection Work Carried Out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence*. Geneva: ICRC.

International Federation of the Red Cross and Red Crescent Societies (IFRC) (2013). *World Disasters Report 2013: Focus on Technology and the Future of Humanitarian Action*. Geneva: IFRC.

Mancini, F., ed. (2013). *New Technology and the Prevention of Violence and Conflict*. New York: International Peace Institute.

Marx, A. and Goward, S. (2013). 'Remote Sensing in Human Rights and International Humanitarian Law Monitoring: Concepts and Methods,' *Geographical Review*, Vol. 103, No. 1, 24 January 2013.

Mattila, M. (2011). *Mobile Technologies for Child Protection: A Briefing Note*. Dakar: UNICEF.

Meier, P. 'iRevolution – from innovations to Revolutions' blog, http://irevolution.net/

Meier, P. (2011). 'New Information Technologies and Their Impact on the Humanitarian Sector,' *International Review of the Red Cross*, Vol.93, No.884, December 2011.

Meier, P. and Leaning, J. (2009). 'Applying Technology to Crisis Mapping and Early Warning in Humanitarian Settings,' Harvard Humanitarian Initiative Working Paper Series, September 2009.

Pierson, L. (2013). 'Elva 2.0 Platform – Forecasting Emerging Security Problems along Georgia's Disputed Border,' 25 March 2013, http://www.statisticsviews.com/details/feature/4528991/Elva-2_0-Platform--Forecasting-Emerging-Security-Problems-along-Georgias-Dispute.html

Save the Children (2012). *Mobile Technology in Emergencies: Efficient Cash Transfer Mechanisms and Effective Two-way Communication with Disaster-affected Communities Using Mobile Phone Technology*. London: Save the Children.

Silverman, C., ed., *The Verification Handbook: A Definitive Guide to Verifying Digital Content for Emergency Coverage.* Netherlands: European Journalism Centre. http://verificationhandbook.com/book/about.php

UNHCR (2013). *Innovation – 2013 Year End Report*. Geneva: UNHCR.

UNICEF (2014). *UNICEF Innovation Annual Report 2014*. New York: UNICEF.

UNOCHA (2013). *Humanitarianism in the Network Age – Including World Humanitarian Data and Trends 2012*. OCHA Policy and Studies Series. New York: OCHA.

UNOCHA (2014). *Unmanned Aerial Vehicles in Humanitarian Response*, OCHA Policy and Studies Series, June 2014.

UN Secretary-General's Independent Expert Advisory Group on a Data Revolution for Sustainable Development (2014). *A World That Counts: Mobilising the Data Revolution for Sustainable Development.* New York: Independent Expert Advisory Group on a Data Revolution for Sustainable Development.

Van der Windt, P. and Humphreys, C. (2012). *Voix des Kivus: Reflections on a Crowdseeding Approach to Conflict Event Data Gathering,* February 2012, http://cu-csds.org/wp-content/uploads/2012/07/Voix-des-Kivus-UBC.pdf.

Voix des Kivus (2011). Voix des Kivus – Project Summary, http://cu-csds.org/wp-content/uploads/2009/10/Voix-des-Kivus-Leaflet.pdf

Wang, B., Raymond, N., Gould, G. and Baker, I. (2013). 'Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities.' *Stability: International Journal of Security & Development,* 2(3): 53, pp. 1-18.

Ziemke, J. (2012). 'Crisis Mapping: The Construction of a New Interdisciplinary Field?' *Journal of Map & Geography Libraries: Advances in Geospatial Information, Collections & Archives*, 8:2, 101-117.

ANNEX I: LIST OF RELEVANT ORGANIZATIONS AND COMMUNITIES OF PRACTICE

The following table lists a number of potential partners or valuable sources of insight and experience and provides relevant website information, where available, found during the course of the research undertaken for this paper. There are undoubtedly others to be added, but this is intended as a starting point for exploring technology-related collaboration and knowledge sharing.

ORGANIZATION	AREAS OF EXPERTISE
Amnesty International USA http://www.amnestyusa.org/research/science-for-human-rights http://www.amnestyusa.org/research/science-for-human-rights/remote-sensing-for-human-rights	Use of satellite imagery and other ICTs for human rights documentation
Build Peace http://howtobuildpeace.org/about-us/	Network bringing together local peacebuilders and technologists to 're-think approaches to early warning and crisis response, attitude and behavior change, collaboration, dialogue, and policy advocacy'

Columbia University – Center for the Study of Development Strategies http://cu-csds.org/ http://cu-csds.org/projects/event-mapping-in-congo/	Crowdseeding
Communicating with Disaster Affected Communities (CDAC) Network http://www.cdacnetwork.org/i/20140728102420-genh0	Convenes humanitarian and media development organisations and technology providers Convening, advocacy, action research and learning, and capacity strengthening on communication as aid
CrisisMappers: The Humanitarian Technology Network http://crisismappers.net/	Information sharing network convening a wide range of UN, NGO, academic and private sector partners and covering a wide range of uses of humanitarian technology for early warning and rapid response to complex humanitarian emergencies
DataKind http://www.datakind.org/howitworks/	Use of data science to support humanitarian initiatives (e.g. analysis of human rights data for early warning and prevention)
Digital Democracy http://www.digital-democracy.org/	Training and tool development Project work on human rights monitoring in Burma and GBV reporting and support in Haiti
DigitalGlobe http://www.digitalglobe.com/	Use of satellite imagery Pattern analysis/predictive analytics [Dr Colleen McCue]
Elva http://www.elva.org/welcome/	SMS reporting and polling Crisis mapping
Esri (ArcGIS) http://www.esri.com/ http://www.esri.com/software/arcgis	Geospatial mapping, visualization and analysis of data Hot spot detection

EyeWitness Project (International Bar Association) http://www.newperimeter.org/our-work/access-to-justice/eyeWitness.html	Secure transmission and verification of photo and video documentation by citizen journalists
FrontlineSMS http://www.frontlinesms.com/	Use of SMS for disseminating and gathering information
Geofeedia http://geofeedia.com/how-it-works	Social media monitoring
Geospatial Technologies and Human Rights Project of the American Association for the Advancement of Science (AAAS) http://www.aaas.org/program/geospatial-technologies-and-human-rights-project	Use of satellite imagery for verification of human rights abuses
Global Education Cluster http://educationcluster.net/topics-lp/information-and-knowledge-management/	Digital data collection Mapping Information management
Ground Truth Initiative http://groundtruthinitiative.org/	Crisis mapping (see 'Map Kibera' project, in particular) Digital data collection
Harvard Humanitarian Initiative – Signal Program on Human Security and Technology http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program	Use of satellite imagery Use of ICTs for human rights documentation
Human Rights Watch http://www.hrw.org	Use of satellite imagery and other ICTs for human rights documentation
Humanitarian OpenStreetMap Team http://hot.openstreetmap.org/	Crisis mapping
Humanitarian Tracker http://www.humanitariantracker.org/	Crisis mapping Data mining tools for searching media reports
IMMAP http://immap.org/	Information management and GIS technology Mapping and visualization of data

Magpi http://home.magpi.com/	Digital data collection Mobile data surveys
Medic Mobile http://medicmobile.org/platform	Tailored mobile platform for collecting healthcare data that can be used in areas with limited or no access to internet and limited electricity
NetHope http://nethope.org/	Network that helps members to collaborate, innovate, and leverage the full potential of information and communications technology to support their causes Connectivity, field capacity-building, emergency response, shared services, innovation for development
Qatari Computing Research Institute – Social Innovation Team http://qcri.com/our-research/social-innovation	Crisis mapping Crowdsourcing AIDR for classifying results of traditional and social media monitoring Verification/credibility of social media Use of satellite imagery

Souktel http://www.souktel.org/development	Mobile data surveys Reporting via SMS Digital data collection
Télécoms Sans Frontières (TSF) http://www.tsfi.org/en	Information systems development Technology access
The Engine Room https://www.theengineroom.org/about/	Support to advocacy initiatives using technology and data in their work
The GDELT Project http://gdeltproject.org/	Real-time data mining of print and online media sources
The Guardian Project https://guardianproject.info/ https://guardianproject.info/informa/	Secure mobile messaging Data security
UN OCHA http://www.unocha.org/what-we-do/information-management/im-services	Crisis mapping Information management Data visualization and analysis

UNICEF (including UNICEF Innovation) http://www.unicef.org/innovation/ http://unicefstories.org/	Digital data collection Information management Crowdsourcing
United States Institute for Peace – Science, Technology and Peacebuilding http://www.usip.org/category/issue-areas/science-technology-and-peacebuilding http://www.usip.org/programs/projects/the-peacetech-lab	Potential uses of technology for peacebuilding and conflict prevention
Ushahidi http://www.ushahidi.com/	Crisis mapping Social media monitoring
Watchlist on Children and Armed Conflict and Permanent Mission of the Principality of Liechtenstein http://watchlist.org/caac-smartphoneapp/overview.html	Mobile phone application on the UN's Children and Armed Conflict agenda 'to provide policy-makers and those seeking to influence them with readily available key documents and appropriate language on child protection issues in order to increase the agenda's impact'

Other useful websites

Clear – Regional Centers for Learning on Evaluation and Results: 'Improved Data Collection Through Mobile-Based Technology'
http://www.theclearinitiative.org/resources-art2.html

Communicating with Disaster Affected Communities (CDAC) Network
http://www.cdacnetwork.org/i/20140728102420-genh0

CrisisMappers: The Humanitarian Technology Network
http://crisismappers.net/

Data-Pop Alliance (Harvard Humanitarian Initiative, MIT Media Lab, ODI)
http://www.datapopalliance.org/welcome

Digital Humanitarian Network
http://digitalhumanitarians.com/

GSMA Disaster Response
http://www.gsma.com/mobilefordevelopment/programmes/disaster-response/programme-overview

ICT4Peace Foundation
http://ict4peace.org/?cat=9

iRevolution: from innovations to Revolutions – blog
http://irevolution.net/

Let Them Talk – blog
http://letthemtalk.org/

Satellite Sentinel Project
http://www.satsentinel.org/

Standby Task Force
http://blog.standbytaskforce.com/

Tech4Relief – blog
http://www.tech4relief.com/

Technology and Human Rights
http://technologyandhumanrights.org/

January 2015