eisf

Managing security-related information: a closer look at incident reporting systems and software

Gonzalo de Palacios

Gonzalo has worked in the aid sector since 1999 in Asian, African, American and European countries as a humanitarian worker, performing a range of technical and coordination positions for several organisations. He has also worked at the headquarters of non-governmental organisations and for the Spanish Cooperation Agency. During the last few years, he has worked in the humanitarian security risk management sector and on the implementation and management of different incident reporting systems. After a short period as consultant, he is now one of the Global Security Advisors at Oxfam.

Introduction

My first deployment to the field as a professional humanitarian worker was in September 1999. At the time, I was 25 and although I had an e-mail account, my head of mission had never seen one. The authorities of the country where I worked had banned the Internet, mobile phones were rare and basic, and information between the field bases and the capital was shared through floppy disks and mail pouches. When I was deployed to the Philippines in November 2013 to respond to Typhoon Haiyan, one of the first services put up by the World Food Program's Logistics Cluster was a satellite Internet connection via a gigantic balloon on the roof of the City Hall of Tacloban. This shows the extent to which information technology has changed in the past decade. Despite some connectivity challenges in certain remote areas, we live in an interconnected world and humanitarian organisations need to share - sometimes sensitive - security-related information between field offices, country offices, regional offices and headquarters.

This article briefly explores the technological platforms non-governmental organisations (NGOs) use to access and share security-related information, particularly focusing on internal incident reporting software. In this article, we also review how organisations can access contextual information to inform security decisions and how organisations use existing external incident reporting technological tools. We will then consider, through four case studies, the technological platforms organisations can use to internally report incidents, highlighting briefly some of the advantages and disadvantages of the systems presented. This article complements the Security Incident Information Management (SIIM) Handbook published by RedR UK, Insecurity Insight and the European Interagency Security Forum (EISF).[1]

Analysis and decision-making

Any guideline about security risk management, whether generic or organisation-specific, highlights the importance of knowing the context of operations to inform location-specific risk assessments and security management plans. Accessing accurate contextual information from both internal and external sources is key to good situational analysis and sound security risk decision-making.

Even when NGO staff have a good knowledge of the context in which they are operating and the organisation has good security risk management systems in place, incidents can still occur. Sometimes it is about being in the wrong place at the wrong time, on other occasions, incidents occur due to external factors or staff negligence, misconduct or other factors. Whatever the cause, when incidents take place, support must be provided as quickly as possible to

1 Redr UK, Insecurity Insight and EISF. (2017). Security Incident Information Management Handbook. Available from: https://www.eisf.eu/library/security-incident-information-management-handbook/. [Accessed 4 Dec. 2017].

victims. Incident reports and the way they are shared are key in this process.

Incident reports provide valuable information about the area in which the incident took place, including whether the victim's profile or actions resulted in the incident occurring, and/or whether the organisation was a direct target. Analysis of the information contained within incident reports should feed into an updated risk assessment and should lead to better informed security decision-making. Incident information management, particularly the analysis of incident-related trends, allows decision-makers to modify security procedures or make operational decisions to mitigate the risk of further incidents occurring, improving the safety and security of their organisation's staff, assets and operations.

Accessing contextual information

Organisations rely on internal and external sources of information to develop strong contextual knowledge of their areas of operation, which directly and indirectly informs NGOs' programmes and security plans. Plenty of contextual information is available through coordination bodies such as the International NGO Safety Organisation (INSO). Many ministries of foreign affairs also offer advice and contextual information on their websites. Online indexes provide information to the public on data related to specific areas, which can help with risk assessments. Organisations can also access useful contextual information through paid services, e.g. through their insurance providers, travel booking services or directly from a company specialising in context analysis.

Additionally, a large quantity of security-related information can be accessed via mobile phone apps. There are apps that connect responders to each other, for example, Humanitarian ID.[2] There are also apps that provide up-to-date humanitarian information, such as the app from the Assessment Capacities Project (ACAPS) or from the Global Disaster Alert and Coordination System (GDACS).[3]

A list of some useful indexes are available in the SIIM Handbook, and additional sources and apps can be found in the 'Further Information' section of this article.

External incident reporting

'Rapid reporting [of incidents] to other agencies in the area is a collective responsibility.'[4]

Usually, when an affiliated organisation suffers an incident, it is reported both internally and externally. Externally it is usually shared through coordination bodies or information sharing initiatives, as well as social media (including, but not limited to, platforms such as Twitter and Facebook).

Coordination platforms such as INSO and the Pakistan Humanitarian Forum share information on incidents in the countries where they work. INSO also provides dynamic statistics, which are updated on a monthly basis on their website, for the contexts in which they are working. The organisation furthermore provides a daily digest of incidents to subscribers called the 'World Alert'. Other very relevant and known organisations that compile information related to security incidents are Humanitarian Outcomes via their Aid Worker Security Database and Insecurity Insight through their Aid in Danger Security in Numbers Database. This data is open source and can be accessed via their respective websites.[5]

In recent years, social media has become a relevant resource to consider when it comes to obtaining or sharing security-related information. Through the search engines of Twitter or Facebook or social media monitoring, an enormous amount of contextual and security information can be found. Social media can also be used to alert others, including groups, about incidents or dangerous situations in a private manner. Facebook has some interesting features, such as 'Safety Check', which lets users tell contacts they are safe and check whether others are well.[6],[7] In addition, 'Community Help' 'lets users ask for and offer help after marking themselves safe during a crisis.'[8]

Another extended method of communication and information sharing is through messaging apps and platforms (e.g. WhatsApp and Skype), but not all of them ensure encryption and privacy in the exchange. This is something that must be considered in contexts where authorities have a record of abuse and control over the population.[9]

2 https://humanitarian.id/. [Accessed 4 Dec. 2017].

3 Regarding the use of instant messaging apps, the ICRC released an article stating the opportunities and risks for humanitarian action in January 2017: ICRC, The Engine Room and Block Party. (2017). *Humanitarian Futures for Messaging Apps.* Available from: http://blogs.icrc.org/new-delhi/wp-content/uploads/sites/93/2017/02/Humanitarian-Futures-for-Messaging-Apps_WEB_.pdf. [Accessed 4 Dec. 2017].

4 Humanitarian Practice Network. (2010). Operational security management in violent environments: Good Practice Review 8, Revised edition. *Overseas Development Institute,* p. 17.

5 The SIIM Handbook provides further information on these and other information sharing platforms.

6 Petronzio, M. (2016). *Facebook's Safety Check feature now rests solely in the hands of its users.* MashableUK. Available from: http://mashable.com/2016/11/17/facebook-safety-check-community-triggered/#Fb08L1KJR5qX. [Accessed 4 Dec. 2017].

7 See https://www.facebook.com/about/safetycheck/. [Accessed 4 Dec. 2017].

8 Petronzio, M. (2016). Available from: http://mashable.com/2016/11/17/facebook-community-help/#B2KkAe0v4EqV

9 Amnesty International. (2016). *How private are your favourite messaging apps?* Available from: https://www.amnesty.org/en/latest/campaigns/2016/10/which-messaging-apps-best-protect-your-privacy/. [Accessed 4 Dec. 2017].

Organisations must also keep in mind that criminals are often skilled in the use of social media and use it to find easy victims. It does not matter if an organisation has a robust security plan if one staff member shares openly via social media details about their next trip.[10]

Internal incident reporting systems and software

Internal incident reporting is part of any sound security risk management system. It is the way organisations know when staff members fall victim to incidents and need support, and when to potentially trigger contingency plans.

There are different types of incident reporting, from an initial phone call or message to a more formal template. The SIIM Handbook provides useful insights and tools for organisations to develop their own system. Whatever system your organisation uses, it is important that incident reports reach those who can provide support as quickly as possible. New technologies can help with this.

All organisations using any type of incident reporting protocol or system, whatever the way information is shared, must keep in mind the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Despite what each member state does, the mentioned General Data Protection Regulation establishes strict requirements for any enterprise, organisation or entity that keeps personal data. Data protection requirements must be considered when designing an incident reporting process and system. Exact requirements will be dependent on an organisation's legal context.

When talking about online systems, there are numerous solutions for this purpose that range from free open source easily self-customisable solutions to tailor-made systems prepared by commercial corporations. According to the organisations interviewed for this article, there are two approaches an NGO can take in using technology to develop an incident reporting system:

1. A stand-alone solution integrated into the servers and systems of the organisation; or
2. 'Software as a Service' where the system is hosted by an external service provider.

No approach is better than the other. The decision on what approach to take will depend on factors such as an organisation's technological strategy and resources, as well as general resources, time, and data protection, among others. Another consideration is that some organisations may be unwilling to hand over control of their incident-related data to an external service provider due to data protection concerns.

There are standard product systems that can be used by an organisation for incident reporting purposes, such as Ushahidi and SharePoint, which are used by ACF-Spain and Christian Aid respectively.[11] Alternatively, the Centre for Safety and Development created a platform, called SIMSON, for NGOs that is now being used by CARE.

SharePoint is a 'web-based application that integrates with Microsoft Office. Launched in 2001, SharePoint is primarily sold as a document management and storage system, but the product is highly configurable and usage varies substantially between organizations.'[12] Although it requires buying a license for its use, some of the Microsoft Office 365 products are free for non-profit organisations. SharePoint is a system that can be used for sharing information in different forms. It is possible to create online forms, which only authorised users can access. One of the great advantages SharePoint has is that as a Microsoft product, it is compatible with data processing software such as Word, Excel, and PowerPoint. This allows an organisation to easily export the data from the system to these applications and share and analyse the information using familiar software.

Ushahidi, the Swahili word for testimony, 'was developed to map reports of violence in Kenya after the post-election violence in 2008.'[13] Staff can send reports via an online form, e-mail, text message or Twitter. Once reports are received, these can be reviewed by an administrator to verify and approve the content, so that they can appear in the map on its main page. Examples of Ushahidi deployments are Syria Tracker[14] or Nepal Monitor.[15] The software is open source and

10 See EISF's guide 'Managing the Message': https://www.eisf.eu/library/managing-the-message-communication-and-media-management-in-a-security-crisis/ [Accessed 28 Nov. 2018].

11 Another piece of software, which is free and open source, is Open Data Kit (ODK), which provides a set of tools that help organisations author, field, and manage mobile data collection. See https://opendatakit.org/. [Accessed 4 Dec. 2017].

12 See https://en.wikipedia.org/wiki/SharePoint [Accessed 4 Dec. 2017].

13 https://www.ushahidi.com/about

14 https://syriatracker.crowdmap.com/

15 https://nepalmonitor.org/

can be downloaded free from the Internet. It needs to be installed in a server so that it can be used online.

The Centre for Safety and Development (CSD) is an organisation that developed a software called SIMSON to allow multiple NGOs to report incidents. SIMSON had an option which allowed users to keep its information confidential or share identified information with other organisations on the system. This system also links with the Insecurity Insight Security in Numbers Database (SiND) which produces regular reports based on NGO incidents and access issues, and thus facilitates easy integration into this global data network.[16] CARE were the only NGO who took up the SIMSON option and have now fully taken over the system.

Alternatively, there are also tailor-made commercial incident reporting systems, which are created to meet the needs of the organisation. World Vision International, for example, uses a tailor-made service, which is hosted by a third party.

Many insurance providers have links with particular service solutions that may be available to customers at a reduced rate and have additional features, such as staff tracking, automatic alerts and travel updates. The recommended service provider will depend on the preferences of the insurance company used and may not best suit the needs of the organisation.

See below a comparison table of the different incident reporting systems referenced here.[17]

There is not one single solution that fits all. One of the keys to success would be choosing the solution that addresses the incident reporting challenges of the organisation proportionally to its size, the available financial and human resources, and perceived future requirements. The solutions mentioned here are described in more detail in the case studies shared in the next section of this article.

Figure 1: Incident reporting systems

	Free	Fee	Open source	Licensed	Stand-alone	Software as a service	Standard	Tailor- made	Integrated graphs
Ushahidi	●		●		●		●		
Open DataKit	●		●		●		●		●
SharePoint		●		●	●	●	●		●
NAVEX Global™		●		●		●		●	●

16 See http://www.insecurityinsight.org/projectshumanitarian.html.

17 See 'Tool 9: SIIM Systems' in the SIIM handbook for further details: https://www.eisf.eu/wp-content/uploads/2017/09/2205-RedR-UK-EISF-Insecurity-Insight-2017-Security-Incident-Information-Management-Handbook-13-Tools-To-Support-Your-Organisation-.pdf [Last Accessed 18 Dec. 2017].

Case Studies

ACF-Spain and Ushahidi

Originally, ACF-Spain received reports by e-mail in a Word template. The security manager then put that information into an Excel spreadsheet and from there produced graphs and statistics about incidents. The process was very inefficient and discouraged field security managers from reporting. They introduced the second version of Ushahidi as an organisational incident reporting system[18] in January 2014 after a process where other systems, new or already in use, were considered.

Ushahidi is an example of free open source software for information collection, visualisation and interactive mapping. Reports can be submitted mainly via an online form, but also through SMS or social media platforms. The report form can be customised so that an organisation can collect the required information, and once reports have been validated it is possible to see them reflected in a map grouped per the pre-defined incident category as defined by the organisation. The platform can be programmed to alert security managers (or others as appropriate) when a new incident has been reported so that they can provide support to the victims and validate the report. And it can also alert other users once the report has been validated. Reported incidents can be viewed individually or filtered by pre-defined incident category or custom fields (e.g. type of victim), which is very useful for briefing purposes and risk analysis. Through Ushahidi, ACF-Spain receives reports via an online form, which can then be displayed as a map according to the number and type of reports submitted. Users can be alerted to incidents being reported through the platform and it is possible to filter and analyse information in a simple and efficient manner.

After ACF-Spain saw the advantages of the system, it was decided later in 2014 to extend the use of Ushahidi to the entire ACF International Network using the third version of the platform, which is more intuitive and ergonomic. At the time of writing, this roll out to the broader network is in a testing phase and about to be launched in the field. Although Ushahidi is a stand-alone solution, the aim is to eventually integrate it with the rest of the systems ACF-Spain uses.

The introduction of Ushahidi as a reporting platform in ACF-Spain meant a clear improvement in incident management. Reporting of incidents increased by 100% compared to the average of the previous years, which was not due to an increase in incidents but rather due to the simplification of the reporting process. This system provides real time statistics of incidents, victims and where incidents are happening most. This has meant that security risk management decisions can be taken more quickly and that the workload related to information sharing has decreased.

Advantages and Disadvantages

The main advantage of Ushahidi is that it can be downloaded at no cost. Installing the system is not too complicated and since the organisation decides where to install the software, data remains under the control of the organisation.

To date, version 2 of Ushahidi is the most suitable to be used as an incident reporting system. Unfortunately, Ushahidi as a company will not develop it further, which could create some issues as other related technologies keep evolving. However, it may be possible for issues to be solved by an organisation's IT staff or for similar systems to be identified.

The main disadvantage of Ushahidi is that statistical representation of the information contained in the database is not integrated into the system, and therefore external solutions have to be combined for this purpose. It is an excellent solution for data collection, but other resources are needed for data analysis.

Introducing Ushahidi as an incident reporting system meant a great improvement for ACF-Spain for two main reasons. Firstly, because the reporting process became more efficient, saving time and improving the security analysis, and secondly because reporting became easier, increasing the number of reports and therefore the possibility to support victims.

18 View the European Interagency Security Forum's Communications Technology Hub article, also written by the author, about the deployment ACF-Spain made of Ushahidi as an incident reporting system: de Palacios, G. (2014). *Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping*. Available from: https://www.eisf.eu/wp-content/uploads/2018/05/2252-EISF-2014-Applicability-of-Open-Source-Systems-Ushahidi-for-Security-Management-Incident-and-Crisis-Mapping.pdf. [Accessed 4 Dec. 2017].

Christian Aid and SharePoint

SharePoint is a web-based team collaboration software tool from Microsoft that can be used for an organisation's document management, intranet and social network, as well as a collaborative software or file hosting service.

Christian Aid directly customised the platform for internal reporting of security incidents. The organisation decided to use SharePoint as an incident reporting platform because of its cost-effectiveness and its compatibility with other Microsoft products. Once an incident is reported through SharePoint, it goes onto a list within the platform. The data collected can easily be exported to Excel, and from there graphs and statistics created. SharePoint itself offers the possibility of visualising data through its Chart Web Parts option, although Christian Aid uses Power BI to collate and map incidents for their reports. Information about how to use the platform is part of the Christian Aid induction process for those who would use the system to report incidents. Additionally, the organisation has guidelines attached to the form providing step by step instructions.

Although it depends on the incident, access to the details of the report is generally limited to the persons affected, the country manager, the regional manager and the Corporate Security Manager. Individuals with permission can access the report, those who have been highlighted in the report can add comments throughout, and if needed, a senior management team member can be assigned to investigate and input their findings to the system.

Regarding the adoption of the platform by the team, the technology does work well, but the main challenge in its use is the limited accessibility by the organisation's wider personnel. From a management point of view, the advantage for Christian Aid of using SharePoint as a platform for the reporting of incidents is that they are able to see which countries have the most incidents month by month. This enables the organisation to concentrate its support on personnel who may need further training or guidance.

Advantages and Disadvantages

Keeping in mind that SharePoint may already be in use by an organisation prior to its consideration as an incident reporting system, its main advantage would be its integration within the system already in use. It would not need the installation of new software or the training of staff on the use of a new platform. The development of the system could be done internally by the IT team already in charge of developing and maintaining SharePoint.

Although it is possible to make surveys with SharePoint, it is not a software designed for reporting or collecting data. Representation of data in a map is not built into the system and would have to be done through the installation of additional software.

It may be a good solution for organisations that find SharePoint effective and do not want to diversify systems, but it needs an IT team familiar with the platform and able to internally support the adaptation and development of the software as an incident reporting tool.

SIMSON: The Centre for Safety and Development and CARE

When this article was originally written, SIMSON was a product of The Centre for Safety and Development (CSD), a Dutch 'non-profit foundation specialised in safety and security for humanitarian and development organisations worldwide.'[19] As such, the Centre for Safety and Development does not implement humanitarian or development aid projects but helps others to do so.

In 2005, CSD created SIMSON, an online incident reporting system that aimed to be a common information sharing platform for NGOs. One of the main differences between independent stand-alone solutions, such as Ushahidi, and SIMSON, is that SIMSON follows the logic of 'software as a service'. NGOs that use SIMSON do not have to install, programme or write the code of any software as this has been done by CSD. Organisations that wanted to use the SIMSON platform hired the services provided by CSD.

While it was intended that SIMSON would provide a platform that allowed multiple NGOs to record and share incident information under a licence agreement, the uptake by NGOs was insufficient to make the platform viable for CSD. As of September 2018, CSD handed SIMSON over to CARE, who now fully own the system and can develop it in the direction they deem most appropriate. SIMSON is now the incident reporting system for the entire CARE network.

SIMSON is an online security incident reporting system where users can see the reported incidents represented on a map. Incidents can be filtered

19 See https://www.centreforsafety.org/home/. [Accessed 4 Dec. 2017].

by category, location and other security-related information. Indicators are developed and users are alerted depending on their profile, each user has different access privileges and the type of information they see on the platform is customisable. Documents can be uploaded to incident reports and the system is built so that the insurance company of the NGO can be made aware of the incident and the support it should provide. SIMSON has been constantly updated, modified and adapted since its launch eleven years ago. Among the current developments is the translation of the platform into other languages such as French and Spanish. SIMSON is not compatible with other systems due to its 'software as a service' nature but SIMSON offers users the opportunity to view statistics directly on the platform and choose exactly what to see.

According to CSD, when they reviewed the management of the system, the challenges did not come from the technological side, but from the 'human factor'. The most important factor for the success of any system is to invest in the training of the end users so they use the system appropriately.

Unlike ACF-Spain when they introduced Ushahidi, one of the main users of SIMSON perceived a decrease in the number of incidents being reported when the platform was opened for use, apparently because it meant some changes in the reporting form and process. However, after this initial drop, reporting increased.

Advantages and Disadvantages

SIMSON was developed as a system that would allow NGOs to share incident information between organisations to improve context understanding and knowledge. Despite a number of NGOs using the SIMSON project, none chose the information sharing option.

SIMSON is linked directly with the Insecurity Insight database so organisations can provide information to the Security in Numbers Database with no additional effort.

An added bonus is that this product was developed specifically for the NGO sector.

World Vision International and NAVEX Global™

World Vision International (WVI), in partnership with the international risk reporting provider NAVEX Global, has created an online incident reporting system for the communication of incidents, grievances, harassment and other events.[20] This system is based on WVI enterprise risk management approach so goes beyond the strict communication of safety and security incidents and encompasses other elements such as corruption, lawsuits and reputation, among others.

NAVEX Global adapts its reporting system to the needs and characteristics of the organisation using it so that clients can highlight what is important for them. The online incident reporting form of WVI is openly available on the Internet.[21] The incident reporting system of NAVEX Global allows input from a variety of sources and all World Vision staff can submit reports on the platform since it serves also as a whistleblowing system. Unlike the other systems analysed, where it is necessary to log in to submit the report, in the case of WVI - NAVEX Global this is not necessary. The data related to the identification of the reporter is provided by the person reporting directly in the web form. The only exception to this requirement is for victims of sexual assault since they need to be protected to the maximum extent possible. The form allows not only directly recruited staff, but suppliers, former employees or external parties to report incidents or events concerning World Vision International. The reporting form and the explanatory guidelines are available in English, French, Spanish and Portuguese. Once the reporting form is filled in, it can be printed or uploaded as a PDF file. Once submitted, the user receives a 'Report Key', allowing reporters to upload documents, view the report later and provide additional information when needed.

In addition to the reporting guideline, NAVEX Global provides its clients with online and in-person training and awareness solutions.

Advantages and Disadvantages

The combination of an incident reporting form, whistleblowing channel and beneficiary complaint mechanism is interesting since it reduces the possible diversity of systems used for similar purposes and ensures all related information is held in one place.

20 See https://worldvision.ethicspointvp.com/custom/worldvision/irf/en/documents/WVI%20QRG%20Incident%20Reporting%20System.pdf. [Accessed 4 Dec. 2017].

21 See https://worldvision.ethicspointvp.com/custom/worldvision/irf/en/form_data.asp. [Accessed 4 Dec. 2017].

Having the support of a company dedicated to ethics and compliance management behind the system can help put incident reporting data alongside other risk management fields.

The form can be quite detailed, which although valuable and interesting, can discourage reporting. It is also likely to be a solution that only financially robust organisations can afford.

Nonetheless, this system presents an innovative approach to incident reporting that is appropriate when approaching security risks as part of a larger risk management architecture. Incident reporting through this channel ultimately requires patience and possibly a higher computer literacy than other systems.

Conclusion

Humanitarian and development organisations are diverse. This diversity is reflected also in the way they approach new technologies and how they manage security-related information and incident reporting in particular.

New technologies can facilitate humanitarian and development work but if the human factor is not aligned with the technological strategy, it may become a burden. New technologies can also support the management of security incidents but must match the capacity and needs of the organisation.

Smaller NGOs with little field presence or those working mainly through partners are likely to benefit less than larger organisations from investing in an online reporting system. Instead, a clear incident reporting process through an e-mail and text reporting template combined with a spreadsheet for graphs and data analysis may be sufficient for this type of organisation.

Medium-sized NGOs with field teams engaged in direct implementation might benefit from the adoption of Ushahidi or the development of SharePoint. These technologies require some time and funding investment but having an electronic system in place can result in a remarkable leap forward in reporting, thereby improving security decision-making and the organisation's ability to support the victims of incidents.

Larger NGOs or international networks would benefit from more adapted solutions and external support would be necessary for them given the complexity of these organisations and their needs, as well as the number of staff and incidents that are likely to occur. For these NGOs, solutions like the ones offered by the Centre for Safety and Development and NAVEX Global (or similar commercial solutions from various risk management companies) could be the most suitable for them.

That said, online reporting systems must be complemented by a robust security risk management framework. Reporting a security incident through an expensive and modern platform is still ineffective if there is no robust response mechanism in place to support victims and later apply lessons learned to inform decision-making and improve staff security.[22]

New technologies should not blur the main objective, which is the safety and security of staff so that they can fulfil their organisational mandates and provide the best support possible to beneficiaries.

22 For more information on the response to and use of security incident information see the SIIM Handbook.

Bibliography and Further Information

Humanitarian Practice Network (2010). Operational security management in violent environments: Good Practice Review 8, Revised edition. *Overseas Development Institute*. Available from: https://reliefweb.int/sites/reliefweb.int/files/resources/B7CC12FDAA7CCCFAC12577F1004A39AF-ODI-HPN_Dec2010.pdf. [Accessed 4 Dec. 2017].

Redr UK, Insecurity Insight and EISF. (2017). Security Incident Information Management Handbook. Available from: https://www.eisf.eu/library/security-incident-information-management-handbook/ [Accessed 4 Dec. 2017].

Security incident information management platforms:

de Palacios, G. (2014). Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping. Available from: https://www.eisf.eu/wp-content/uploads/2018/05/2252-EISF-2014-Applicability-of-Open-Source-Systems-Ushahidi-for-Security-Management-Incident-and-Crisis-Mapping.pdf. [Accessed 4 Dec. 2017}.

OpenDataKit. https://opendatakit.org/ [Accessed 7 Dec. 2017].

About Ushahidi. https://www.ushahidi.com/about [Accessed 7 Dec. 2017].

https://en.wikipedia.org/wiki/SharePoint [Accessed 7 Dec. 2017].

World Vision International Incident Report Form. https://worldvision.ethicspointvp.com/custom/worldvision/irf/en/form_data.asp. [Accessed 7 Dec. 2017].

General and security contextual information:

Canadian Ministry of Foreign Affairs. http://international.gc.ca/world-monde/country-pays/index.aspx?lang=eng [Accessed 4 Dec. 2017].

French Ministry of Foreign Affairs. http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/conseils-par-pays/ [Accessed 4 Dec. 2017].

Spanish Ministry of Foreign Affairs. http://www.exteriores.gob.es/Portal/es/ServiciosAlCiudadano/SiViajasAlExtranjero/Paginas/RecomendacionesDeViaje.aspx [Accessed 4 Dec. 2017].

United Kingdom Ministry of Foreign Affairs. https://www.gov.uk/foreign-travel-advice. [Accessed 4 Dec. 2017].

United States Department of State. https://travel.state.gov/content/passports/en/alertswarnings.html [Accessed 4 Dec. 2017].

Information about the humanitarian context:

Assessment Capacities Project (ACAPS). https://www.acaps.org/. [Accessed 4 Dec. 2017].

Humanitarian Data Exchange. https://data.humdata.org/ [Accessed 4 Dec. 2017].

Humanitarian Response. https://www.humanitarianresponse.info/ [Accessed 4 Dec. 2017].

Index for Risk Management. http://www.inform-index.org/ [Accessed 4 Dec. 2017].

Irin. https://www.irinnews.org/ [Accessed 4 Dec. 2017].

RedHum. http://www.redhum.org/ [Accessed 4 Dec. 2017].

Reliefweb. http://reliefweb.int/ [Accessed 4 Dec. 2017].

Indexes and dynamic maps:

Fragile States Index. http://foreignpolicy.com/fragile-states-2014/#rankings [Accessed 4 Dec. 2017].

Global Disaster Alert and Coordination System. http://www.gdacs.org/ [Accessed 4 Dec. 2017].

Global Incident Map. http://www.globalincidentmap.com/map.php [Accessed 4 Dec. 2017].

Global Peace and Terrorism Index. http://www.visionofhumanity.org/# [Accessed 4 Dec. 2017].

Homicide Monitor. http://homicide.igarape.org.br/ [Accessed 4 Dec. 2017].

Liveuamap. http://liveuamap.com/ [Accessed 4 Dec. 2017].

Roads Kill Map. http://roadskillmap.com/ [Accessed 4 Dec. 2017].

Apps:

Headlines and Crises by ReliefWeb. http://labs.reliefweb.int/apps [Accessed 4 Dec. 2017].

iGDACS by the Global Disaster Alert and Coordination System. https://itunes.apple.com/us/app/igdacs/id511250025?ls=1&mt=8 [Accessed 4 Dec. 2017].

Kiosk by Humanitarian Response. https://www.humanitarianresponse.info/en/applications/tools/category/humanitarian-kiosk [Accessed 4 Dec. 2017].

Relief Central by Relief Central. https://itunes.apple.com/us/app/relief-central/id353219185?mt=8 [Accessed 4 Dec. 2017].

Umbrella by Security First. https://secfirst.org/ [Accessed 4 Dec. 2017].

Websites consulted for the article:

Amnesty International. (2016). *How private are your favourite messaging apps?* Available from: https://www.amnesty.org/en/latest/campaigns/2016/10/which-messaging-apps-best-protect-your-privacy/. [Accessed 4 Dec. 2017].

Avakian, C. (2014). 5 mobile apps for humanitarian workers. *Social Brite.* Available from: http://www.socialbrite.org/2014/01/16/mobile-apps-for-humanitarian-aid-workers/ [Accessed 4 Dec. 2017].

EUR-Lex. http://eur-lex.europa.eu/homepage.html [Accessed 7 Dec. 2017].

Facebook Safety Check. https://www.facebook.com/about/safetycheck/. [Accessed 4 Dec. 2017].

ICRC, The Engine Room and Block Party. (2017). Humanitarian Futures for Messaging Apps. Available from: http://blogs.icrc.org/new-delhi/wp-content/uploads/sites/93/2017/02/Humanitarian-Futures-for-Messaging-Apps_WEB_.pdf. [Accessed 4 Dec. 2017].

International Non-Governmental Organisation Safety Organisation's Dashboard. http://www.ngosafety.org/keydata-dashboard/ [Accessed 4 Dec. 2017].

Petronzio, M. (2016). Facebook's Safety Check feature now rests solely in the hands of its users. *MashableUK.* Available from: http://mashable.com/2016/11/17/facebook-safety-check-community-triggered/#Fb08L1KJR5qX. [Accessed 4 Dec. 2017].

Villarino, E. (2015). 7 mobile apps for humanitarians. *Devex*: https://www.devex.com/news/7-mobile-apps-for-humanitarians-85431 [Accessed 4 Dec. 2017].

Acknowledgements

The author and EISF would like to thank the following individuals who have contributed their experience to inform this article:

Álvaro Villanueva (Logistics and IT Director at ACF-Spain),

Ebe Brons (Director of the Centre for Safety and Development),

Rob Treffens (Safety and Security Group Coordinator, CARE International)

Andrew Kirkham (Corporate Security Manager, Christian Aid), and

Christina Wille (Co-Director, Insecurity Insight).

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points, who currently represent over 90 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Federal Department of Foreign Affairs (FDFA), the Department for International Development (DFID) and member contributions.

www.eisf.eu

About the Communications Technology and Security Risk Management Hub

The Communications Technology and Security Risk Management Hub is a project by EISF that was launched in October 2014. The project aims to begin a conversation towards a better understanding of the specific nature of the security threats created by the digital revolution, and the implications for the security risk management of humanitarian staff and programmes.

The first publication of this project (October 2014) brought together 17 authors who analysed in 11 articles how communications technology is changing the operational environment, the ways in which communications technology is creating new opportunities for humanitarian agencies to respond to emergencies, and the impact that new programmes have on how we manage security.

The hub aims to provide an outlet for researchers and practitioners to make original and policy-relevant research available to the humanitarian community. Each article is reviewed by experts. If you would like to contribute please contact the editor of the series at eisf-research@eisf.eu.

https://www.eisf.eu/theme/communications-technology-and-humanitarian-delivery/

Disclaimer