# LIVES ON THE LINE

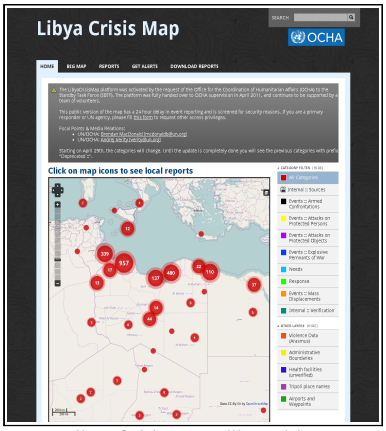
## Securing Crisis Maps in Libya, Sudan, and Pakistan

george chamales – rogue genius llc – george@roguegenius.com

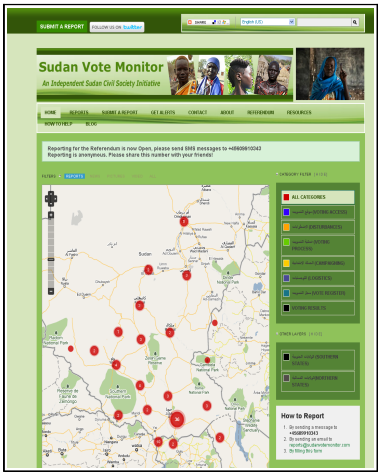
Crisis maps are used to collect and present open source intelligence (Twitter, Facebook, YouTube, news reports) and direct messages (SMS, email) during disasters such as the Haiti earthquake and ongoing civil unrest in Africa. While the deployment of crisis mapping technology is on its way to becoming a standard tool to collect and track ground truth from crisis zones, very little work has been done to evaluate and mitigate the security challenges involved in the technology's deployment.

With active deployments taking place in countries such as Libya, Sudan, and Egypt, there is a growing possibility that the information on these platforms could be utilized for malicious purposes. It is imperative that the vulnerabilities in this technology and deployments be understood and mitigated through the development of standards and best practices.

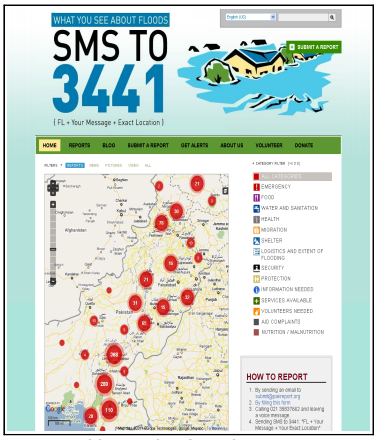
This paper introduces crisis mapping and utilizes examples drawn from real-world deployments to identify vulnerabilities that can be used in the development of security standards and best practices. These concepts are intended to help lay the foundation for methods to secure crisis mapping deployments, and help protect the people they serve when used in hostile environments.




UN's Libya Crisis Map: libyacrisismap.net




Sudan Vote Monitor: sudanvotemonitor.com

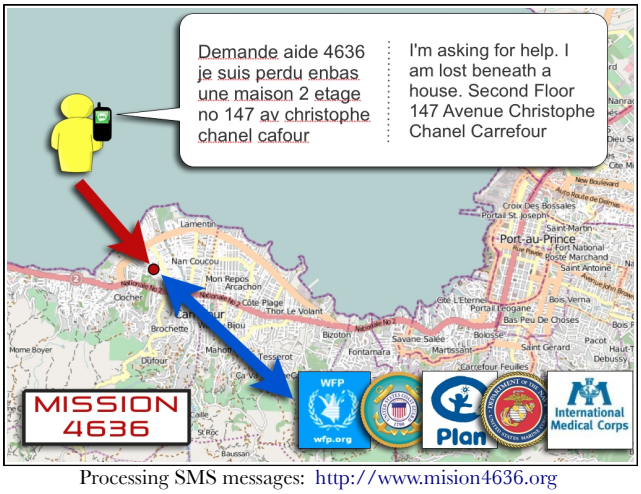



Pakistan Flood:s pakreport.org

## Humanitarian technology is at a crossroads

New technologies like cellular phones and the Internet challenge the traditional one-way flow of information and services that response organizations are used to providing. It is now possible for the citizens on the ground in an emergency to broadcast a wealth of information from the effected area. Choosing to embrace these new communication technologies can enable response groups to rapidly develop situational awareness, build trusted reporters on the ground to verify and validate information, and provide much more targeted aid to those in need. Systems to implement that collection process are under active development and have already seen use in the field.

Port Au Prince, Haiti: http://news.bbc.co.uk/2/hi/8460574.stm




Processing SMS messages: http://www.mision4636.org

Days after a 7.0 magnitude earthquake decimated the capital city of Haiti, a small team of technologists acquired the SMS shortcode 4636 and published the number throughout the disaster affected area. The project, which came to be known as Mission 4636 [1], received over 50,000 SMS messages from citizens on the ground - messages containing calls for help from newly formed camps in open spaces such as sports fields and the locations of people trapped inside buildings. The messages, most of which were received in Haitian Kreyol, were translated by an online team of over 1000 members of the Haitian diaspora collected through Facebook, then geolocated by additional online volunteers to pinpoint the location where the messages originated. The processed messages were then forwarded to relief agencies on the ground including the US Coast Guard, FEMA, and other organizations. Those reports enabled the response agencies to develop situational awareness on the ground and determine where aid was most needed.

This approach, the collection and processing of messages from the ground using teams on the Internet and online platforms, is referred to as crisis mapping. In the eighteen months since the Haiti earthquake, the concept has been adopted and adapted by a variety of organizations performing deployments ranging from natural disasters, to contested elections, to tracking violence in active war zones.

## Natural Disasters Don't Shoot Back

Deploying crisis maps in natural disasters is relatively straightforward - information from the ground can be used to support aid activities for the expected health and humanitarian challenges resulting from that disaster. The use of that same technology in conflict zones, or areas with one or more active hostile groups, significantly changes that dynamic by introducing an unpredictable element of danger that can be difficult or impossible to anticipate and adapt to.

Crisis mapping technology is now being actively used in hostile environments around the world. Those deployments have faced a variety of challenges in maintaining the security of their operations.

> **Pakistan** - During the nation-wide flooding in 2010, the Taliban announced that they would attack foreign aid workers inside the country [2]. A team operating the Pakreport.org crisis map in Pakistan, which included the locations of foreign aid workers, needed to rapidly adapt their approach to avoid the possibility that their data could be used to target response agency personnel.
>
> **Sudan** - A crisis map monitoring the voting stations for a nation-wide referendum received blatantly false reports and had their server blocked from being accessed by those inside the country [3].
>
> **Egypt** - Members of the Egyptian security services demanded that they be given a username and password to the backend of the crisis mapping system designed to monitor polling stations during the country's elections in late 2010 [4].
>
> **Libya** - The United Nations requested a crisis map to monitor the escalating violence in Libya in order to provide them with an understanding of what was happening in key areas throughout the country. The deployment administrators restricted access to the collected data and analysis to prevent it from being used by hostile forces on the ground and minimize the possibility that a compromise of the platform could be used to target the aid agencies using that information [5].

The use of crisis mapping technology is in part driven by new tools and hosted solutions that are making it easier to deploy and manage crisis mapping systems [6]. As the technology becomes more readily available to activists and organizations around the world it can be expected that these deployments will continue to be used in the field, drawing further attention from hostile organizations.

## Vulnerabilities of Crisis Maps

Crisis mapping technology presents a series of unique operational security challenges that must be overcome to ensure that the deployment remains functional and the information it collects is not manipulated or misused. While the situations and locations where crisis mapping technology can be utilized vary widely, there are a number of steps that must be taken by each deployment. By examining those steps it is possible to identify the types of vulnerabilities and begin to develop mitigation procedures that can reduce the potential for successful attacks.

### Implementing Organization

Currently, choosing the lead crisis map deployment for a given crisis is an ad hoc process, with the larger crisis mapping community supporting whichever group sets one up first and appears to have the most momentum. As the technology needed to implement crisis maps gets easier to deploy it is less likely that the first mover will be the same as the organization best suited to manage the many complex decisions and security procedures needed to operate a deployment. Furthermore, it can be difficult or impossible to verify the identify or group affiliations of the person or persons deploying a given map.

### Choice of Platform

The fundamental capabilities needed by a crisis mapping platform - message collection, curation, and presentation, can be implemented by a variety of different software platforms. These platforms range from commercial products, online services, and dedicated open source projects such as Ushahidi [7] and Sahana [8]. On several occasions such as the nuclear disaster in Fukushima [9], platforms have been built from scratch. From a security standpoint, each of these approaches have their strengths and weaknesses - bugs in commercial platforms may require vendor patches, online services cannot be easily tailored to a particular deployment, and open source projects may not focus on security over core functionality.

### Location of Platform

Placing the platform online broadens the organizations and people it can reach but opens it up to attack from the Internet. The choice of network also influences the ability of the system to be monitored and blocked. Placing it inside the crisis zone opens the possibility for physical attacks and that the platform could be cut off from the Internet if network connectivity in that area is disabled. Placing it outside the conflict zone means that those on the ground may be unable to access the information if their Internet access is blocked.

### Message Collection

Collecting usable reports from the ground is one of the most challenging components of any crisis mapping deployment. It is also the part of the deployment where those on the ground can become potential targets by providing information on what it is they are

seeing around them. Messages to public sources such as YouTube, Twitter, and mainstream media reports can be intercepted or blocked by those who control the network. Identifying trustworthy, reliable sources is an ongoing challenge, and the more useful a reporter is to a given deployment by providing high quality information, the higher profile they may become for targeting.

### Message Processing

Crisis mapping deployments may collect thousands of messages that must be translated, categorized, geolocated, and verified before they can be shared with users of the platform. These steps can be partially automated, but human analysts are still needed to perform quality control and to handle tasks, such as translating slang language from text messages or geolocating places that do not exist in online databases.

Current approaches utilize groups of volunteers sourced from the Internet. Giving strangers direct access to the message processing can enable bad actors to delete messages, compromise reporter's identities, and lead to incorrect results. Microtasking systems, that separate the processing of messages into discrete tasks can mitigate the exposure of information and make it possible to require agreement between analysts on things like location and category before the message is marked for publication. Groups dedicated to supporting crisis mapping deployments such as the Standby Task Force [10] or Crisis Mappers.net [11] can provide trained personnel, but perform only basic background checks on new volunteers.

### Presentation of Reports

The final step in the reporting process is the decision to make reports available to those utilizing the platform. The finished reports can be utilized by response organizations to identify where aid is needed or by hostile groups to target vulnerable populations. Various strategies exist to mitigate these threats, ranging from private deployments where only approved organizations have access, semi-private deployments which only provide public access to already publicly available information, and redacted deployments where sensitive information has been stripped from the public reports but the full information is still available to a trusted organizations.

## Towards Best Practices in Crisis Mapping Security

Crisis mapping is increasingly being used as a tool to track events in hostile environments. Along with that growth comes increased scrutiny from organizations that the technology threatens. With existing actions taken by government security forces and the ongoing harassment and threats against those who report on what they see, there is a growing need for a body of standards and best practices that those deploying this technology.

Developing those standards will require a collaboration between experienced members of the security community and those leading the crisis mapping movement. The development of those standards will be challenged by the breadth of situations where this technology can be utilized and the variety of threats that a deployment may face. This process can be streamlined by focusing on the steps that must be taken in every deployment such as those listed above, enabling those working with this technology to obtain guidance for each step of their deployment.

Establishing security standards is by no means a guarantee that negative consequences from a crisis mapping deployment will be prevented - mistakes will always be made under stressful circumstances and new attacks and vulnerabilities will be developed by sophisticated attackers. When that does take place, having established a baseline for the secure use of this technology will provide a way to quickly incorporate new procedures. This body of security standards and best practices will provide the humanitarian technology community with the knowledge they need to keep themselves, their deployments, and their users safe.

## References


[1] Mission 4636: http://www.mission4636.org
[2] Taliban Threatens Pakistan Aid Workers
http://www.washingtontimes.com/news/2010/aug/26/taliban-threatens-foreign-aid-workers/
[3] Dealing with Dirty Data: The Sudan Vote Monitor Deployment
http://blog.ushahidi.com/index.php/2011/07/01/dealing-with-dirty-data-the-sudan-votemonitor-project/
[4] How Egyptian Activists Kept Their Ushahidi Project Alive Under Mubarak:
http://irevolution.net/2011/05/25/u-shahid-interviews/
[5] Academics Join Relief Efforts Around the World as Crisis Mappers
http://chronicle.com/article/Academics-Join-Relief-Efforts/126912/
[6] Crowdmap: http://crowdmap.com
[7] Ushahidi: http://ushahidi.com
[8] Sahana: http://sahanafoundation.org
[9] Fukushima: http://rdtn.org
[10] Standby Task Force: http://blog.standbytaskforce.com
[11] CrisisMappers.net: http://crisismappers.net


## About the Author


George Chamales has spent the last decade working in almost every legal permutation of employer and job the computer security field has to offer. His list of current and former government employers includes DOD, DOE, DHS, and DOI. In the private sector, he's worked as a security architect, member of the Honeynet Project, and corporate pen-tester targeting Fortune 500 companies. He is an active member of the crisis mapping community, where he develops new tools and capabilities, co-founded of the Crisis Mappers Standby Task Force, and has served as the technical lead for numerous deployments including LibyaCrisisMap.net, Pakreport.org, and SudanVoteMonitor.com. He can be reached at george@roguegenius.com