EUROPEAN ACADEMIC RESEARCH
Vol. IV, Issue 4/ July 2016

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Crowd-sourced Crisis Data: Ethical and Legal Concerns

BUDDHADEB HALDER
Universitat Autònoma de Barcelona
Barcelona, Spain

Abstract:

Crisis informatics is now based on crowdsourced data analytics- a combination of crowdsourcing retrieval and filtering, and decision support systems. Digital volunteers are using machines to achieve real-time data analytics. Along with providing information, volunteers also participate in collective task-solving requests. Digital humanitarian networks offer the task of data analysis to volunteer communities. In near future, more accurate digital data i.e. image, geo-location and text, collected through excellent techniques like sensors system, GPS, UAV or satellite, will definitely make tasks more effective. However, there will be more risks as we use emerging communication tools and methods for disaster response management works. This paper is going to be based on identifying some ethical and legal concerns in crowdsourcing crisis informatics. Some possible solutions for disaster response platforms' management contributing to Disaster Risk Reduction will also be proposed.

Key words: Crowdsourcing, Crisis management, Crisis Informatics, Crowdsourced Data Analytics, Situational Awareness, Decision Making Support Systems, Disaster Risk Reduction.

Categories and Subject Descriptors

H.3.5 [Online Information Services]: *Web-based services, Data sharing*. K.4.1. [Public Policy Issues]: *Abuse and crime involving computers, Ethics, Human safety, Privacy, Regulation, Transborder data flow Use/abuse of power*. K.5.2 [Governmental Issues]: *Regulation*

General Terms
Management, Measurement, Documentation, Security, Human Factors, Standardization, Legal Aspects, Verification.

INTRODUCTION: GENERAL CONCERNS

The final outcomes of the Third United Nations World Conference on Disaster Risk held in March 2015, the Sendai Framework for Disaster Risk Reduction 2015-2030, adopted a 'concise, focused, forward-looking and action oriented Post-2015 framework for disaster risk reduction [1]. This framework neither used a single word on the role of emerging ICTs in disaster risk reduction nor the potential risks of disaster response workers or volunteers. However, some indirect references to disaster management and response were made. In 2005, The Hyogo Framework for Action (HFA1) settled the disaster risk reduction principles. The United Nations Office for Disaster Risk Reduction (UNISDR) will have to update them in 2016. Risk identification and reduction, disaster response and adaptive governance converge, and crisis informatics plays a relevant role in the disaster management system.

One of the most exciting contributions of ICTs in disaster response coordination work is the use of ICT-based crowdsourcing and crisis mapping. Though, some risks have been identified which are associated with this approach:

A. **Security breach due to system malfunction or insecure data transmission**: OCHA (2014) identifies, 'as more data systems and devices go online, there has been an explosion of cyber-crime, as well as cyber-warfare'. Using crowdsourcing in humanitarian crisis management could create risks like attacks on communities like 'aid recipients, such as marginalized groups or displaced people' or groups; attacks on humanitarian partners and this type of attacks could come from terrorist organisations, opposition groups engaged in conflicts etc. 'This motive could be linked to a conflict or political dispute,

religious or ethnic tensions, or social mores, such as targeting women who report sexual or gender- based violence' (OCHA 2014). According to OCHA (2014) perpetrator groups may find 'humanitarian organizations as a soft point of entry to government or commercial data sets or networks'. As humanitarian organizations begin using ICT-based crowdsourcing tools and procedures, more sophisticated communication systems and internet-linked tools, cyber-attacks are becoming really easy for perpetrators. Failure to understand these challenges can put victims and others directly at risk that is more than enough to damage the trust humanitarian organizations require doing their work [2].

B. Personal information disclosure, location data management, sensitive data (health, political opinion and etc.), quality of data and discrimination: Using crowdsourcing process in humanitarian crisis management means dealing with information, personal data and even sensitive data like health or ethnic origins or sexual orientation and etc. Privacy might thus be at risk due to the crowdsourced response platforms involved in the disaster management. The general principles of Fair Information Practice (FIP) and EU data protection should be preserved when using crisis informatics. For instance, improving the data quality (data format, taxonomy, clarity, etc.) in disaster response operation is must. On the other hand, if crisis responders, researchers and academia fail to develop proper standards, guidelines and practices to facilitate the exchange and transferability of data between groups and individuals, this will also add further risks. C. Lack of coordination: Another important risk in crowdsourcing for humanitarian crisis management is the absence of a common mechanism specifically designed for collaboration and coordination between different agencies working for disaster response cause [3]. Also a common platform for humanitarian crisis response coordination work among different stakeholders engaged in crisis response management work is missing. Using crowdsourcing for

humanitarian crisis management would not get the optimum response without such type common platform for collaboration and coordination. The United Nations suggested as 'several actors including NATO, OGC, ISPRS and GEO are working on similar issues and could be integrated in a concerted effort' [4].

D. False positives, automatic decision-making: Last but not least, decision support systems soon will replace volunteers as a source of information, selection and response teams' support. These automatic decision support tools will generate a number of false positives and might in some cases even substitute expert's decision-making. However, in the legal field, a decision cannot be solely based on automatic tools. This general principle shall also apply for crisis informatics.

As some risks have already been identified, it is time to take a look how they are linked with the tasks conducted by online volunteers in crisis management:

A. Data retrieval and selection: Collection and filtering can be done by digital volunteers. They contribute in achieving collective task solving and crisis mapping. It can also be implemented by using data analytics, like social network analysis, user ranking, machine learning, sensors and ultimate meta-data crisis mapping. However, security and privacy risks re very much associated with data retrieval and selection processes.

B. Situational awareness: On the other hand, situational awareness is offered by human sensors, support teams and humanitarian networks. Now, digital volunteers are more organized than in the past. But these networks trigger new risks. Coordination between response teams and digital volunteers, and also ad hoc solution teams created by digital communities are the risks related to situational awareness tasks.

C. Decision support: The last group of tasks involves decision-making support: OCHA and the Digital Humanitarian Network coordinate to offer decision support. This can be considered as coordination risk. On the contrary, simulation,

geomatics and emotion classification will become a decision support tool for response teams very soon. It is at this stage when false positives might be more dangerous.

PROBLEM STATEMENT

The explosive growth of information technologies across the world has given enormous power to the hands of common people. Though, different positive aspects of crowdsourcing have already been recognized, serious concerns have also been raised in terms of privacy, security and personal data protection in using crowdsourcing during any crisis events. Thus, a research has been conducted on numbers of crowdsourcing crisis management platforms to understand some ethical and legal concerns in crowdsourcing crisis informatics.

RESEARCH QUESTION

The following main research question has guided the research work on different crowdsourcing platforms. Thus, this same would guide this research article:

> *What are the different privacy, security and data protection issues associated in using crowdsourcing for crisis management?*

RESEARCH METHODOLOGY

There are three different stages in using crowdsourcing platforms for crisis management. The stages are a) Retrieval and Selection (RS); b) Situational Awareness (SA); and c) Decision Support Systems (DSS). During the literature review it has also been identified that there are 71 different security, privacy and data protection components[1] are linked with these

[1] 40 different risks for Retrieval and Selection (RS); 20 different risks for Situational Awareness (SA); and 11 different risks for Decision Support Systems (DSS).

three stages when crisis coordinators use cowdsourcing for crisis management. Based on these 71 privacy, security and data protection components, an intensive secondary research has been completed. To understand these aspects within existing different crowdsourcing crisis management framework, a qualitative research study was conducted among Uhahidi, Digital Humanitarian Network, MicroMappers and Google Crisis Map.

Identification of crowdsourcing tools

Ushahidi

Ushahidi (USH) has been identified for secondary research as this platform is considered as the pioneer and innovative crowdsourcing platform that paved the way for using ICT based crowdsourcing in crisis management works. Ushahidi first started its groundbreaking work with the deployment of an innovative crowdsourcing platform to monitor incidents of post-election violence in Kenya in 2008 and peace efforts throughout the country based on reports submitted via the web and mobile phones. Platforms like Ushahidi and its' sister platforms like SwiftRiver and Crowdmap offer volunteers and other users to create "reports" from social media updates, direct information and conventional media activities accompanied by GPS location for the report when available and possible. In Ushahidi, volunteers and users can track their reports on the map. And they can filter their data by time, and see when things happened and where. This platform allows users to collect information via text messages, email, twitter and web-forms. Ushahidi has recently developed another 'check-in tool' called 'Ping' that would support crisis management works using crowdsourcing by adding users' contacts to a group helping anyone to 'Ping multiple people with the push of a button'. This

tool can 'create and store contacts with multiple numbers and email addresses for each for multiple points of contact'[2].

Digital Humanitarian Network (DHN)

There are numbers of networks that voluntarily work to address different crisis situations. As the Digital Humanitarian Network (DHNetwork) is the network of Volunteer & Technical Communities of its' kind to leverage digital networks in support of humanitarian response, it has been identified for the secondary research. The aim of this platform is to "provide an interface between formal, professional humanitarian organizations and informal yet skilled-and-agile volunteer & technical networks". DHN use different tools to address crisis issues. Some examples are the Humanitarian UAV Network (UAViators) or Planetary Response Network for crowdsourcing satellite imagery analysis for humanitarian response. Humanity Road has also worked under the Digital Humanitarian Network's Solution Team to build up a Situation Report for OCHA's team in the Philippines. Some DHNetwork Coordinators are in charge of contacting volunteers and technical teams' members of Digital Humanitarians to build a Solution Team for particular requests. DHN uses different tools while working towards managing a crisis. For example, DHN uses 'Verily' that collects crowdsourced evidence, and provide important information for crisis responses. In the present 'Disinformation Age', finding the truth in the huge amount of contradictory and confusing information is becoming increasingly difficult for crisis responders. Verily is an experimental web tool designed to rapidly share verified information during humanitarian disasters, it uses a time-critical crowdsourcing process to verify information during major disasters on behalf of humanitarian organizations and media groups.

[2] To know more about 'Ping' visit http://bit.ly/1RNl5dW

MicroMappers

The platform 'MicroMappers'(MM) has been identified for the research as it has started AI (Artificial Intelligence) for the first time to select data and information by users. It is a collection of websites or Clickers (beta version) and each clicker or volunteer can easily tag different types of information. There are several categories of digital volunteers associated with MicroMappers[3]. 'Text Clickers' for instance identify the relevance of Tweets during an emergency or disaster. 'Image Clickers' are volunteers who rate the damage by looking at images. These volunteers check, verify and rate different crowdsourced information and data and then the platform passes that information to 'Geo Clickers' who put those tweets, pictures and videos on the map. In the recent earthquake in Nepal in May 2015, over 2800 volunteers from all over the world reviewed tweets and images to support humanitarians with information insights. These 'clicks' and 'selections' of texts by volunteers produced a highly accurate dataset about the earthquakes in Nepal that was shared and incorporated into the damage assessment and decision-making processes. At the end of the process, some empowered group of volunteers inserted the gathered information on a map, where the type and seriousness of incidents are reported. At this stage the support teams and the decision makers' work together to accelerate the crisis management. MicroMappers is using AIDR (Artificial Intelligence for Disaster Response) - an artificial intelligence engine developed to power consumer applications like MicroMappers. This platform permits humans and machines to work together to apply human intelligence to large-scale data at high speed. Meier (2013) has identified that 'the free and open source Artificial Intelligence for Disaster Response platform

[3] Volunteer categories are 1. 'Text Clickers' for Tweets, 2.'Image Clickers' for Pictures, 3. 'Aerial Clickers' for Aerial Pictures, 4. 'Video Clickers' to tag videos and finally, 5. 'Geo Clickers' to map tweets, pictures and videos. There will be another category called 'Translate Clickers' to crowdsource the translation of tweets very soon.

leverages machine learning to automatically identify informative content on Twitter during disasters'.

Google Crisis Map

Google Crisis Map (GCM) has been selected for this research to identify, having all latest technological facilities, how does it care about privacy, security and data protection issues. Google has been responding to natural disasters since Hurricane Katrina in 2005 by making information such as storm paths, shelter locations, emergency numbers, and donation opportunities easily accessible. Only after mid 2012 Google has started creating Crisis Maps. Google Crisis Map is a collection of national and regional-scale layers related to weather, hazards, and emergency preparedness and response, mostly for the US. Google has developed several tools to help responders to achieve their goals in crisis situations. For example, Google Public Alerts, Google Person Finder, Google Maps Engine Lite, Google Earth etc. First responders can use these tools to streamline internal operations and get information to the public as quickly, broadly, and effectively as possible.[4]

RESEARH OUTCOME

There are numbers of different activities have been identified that have been executed during the three different stages i.e. a) Retrieval and Selection (RS); b) Situational Awareness (SA); and c) Decision Support Systems (DSS). The identified risks will be mentioned below in from 5.1 to 5.3.

Data retrieval and selection concerns

Until 2010, crowdsourcing was mainly based on retrieval and selection of data. Current crisis crowdsourcing platforms suggest collective task solving for volunteers. Some disaster

[4] To know more visit http://www.google.org/crisisresponse/

response networks like Digital Humanitarian Network (DHN) offer these resulting tools to volunteer communities and response teams. In sum, crowdsourcing remains a source of information, but is quickly becoming a training procedure for data analytics. These complex disaster management networks need to preserve security and privacy, not only for the traditional crowdsourcing of data, but also for new automatic retrieval and selection capabilities.

Collective task-solving and mapping

Upon filtering the relevant data, crowdsourcing crisis informatics has proved to be useful for response teams. Only near-real-time and highly accurate information is required for response teams. Duplicate reports and unavailability of essential information are added problems for response teams [5]. Crowdsourcing crisis mappers want to offer useful and relevant information, which also needs to be identified as trustworthy partner in officially decision-making process for emergency management. Most of the crisis-mapping deployments lack enough accuracy of crowdsourced data compared with more 'traditional data'. The quality of data from 2008 to 2011 has shifted from trustworthiness to "good enough" [6]. More recently, crisis informatics based on data analytics offer new trust options. Some risks are also due to the absence of data validation from end-users, gaps in reporting back on on-going emergencies and lack of publicity of crowdsourcing activities [4]. There are ways to minimize those risks. Firstly, filtering the data, i.e. asking where the information originates from. Secondly, cross checking the collected data with other data sources. Thirdly, by setting up a framework where the crowd verifies the crowd, respecting transparency and open data policies and practices [4].

Inaccuracy and bellow quality of data are not only crisis mapping risks; security needs also to be preserved. Recent studies suggest that humanitarian organisations have a long way to go to ensure a sufficient level of technical security

against cyber-attacks [7]. The same applies in using crowdsourcing tools or methodologies for humanitarian crisis management as well. Gao et al. [5] suggest that crowdsourcing tools for crisis response management do not have adequate security features for users and reporters, registered users, relief organizations, and relief operations. Online activities of humanitarian organisations are highly vulnerable to cyber-attacks [8].There are reliable reports of human rights activists and other 'people communicating with humanitarian organisations over Skype being tortured to give up their passwords, with their accounts then used to transmit malware to NGO staff and their contact networks' [8, 9]. Different social media page of the International Secretariat of Amnesty International faced nuisance cyber-attacks in 2011 by Syrian Electronic Army. One of the several examples is the nuisance attack was on a crowdmap platform that was developed by the Amnesty International. Syrian Electronic Army used to send spams in every other minute.[5] The same 'Syrian Electronic Army' did the same to Human Rights Watch [10]. In the case of crowdsourcing for humanitarian crisis management, 'attempts to steal data or to spy on a target are probably the greatest concern since they can endanger assisted people and aid workers' [2]. Another risk of using crowdsourcing for humanitarian crisis management is that in the present 'network-age', governments have access to sophisticated interception and surveillance software[6]. Thus, all these facts pose difficult challenges for humanitarian crisis response

[5] This was the personal experience of this researcher as he was then employed at the IS as an Online Communities Officer.

[6] The Blue Coat Packetshaper, a type of malware used for this type of surveillance, was found in Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela, according to research done by the Citizen Lab at the University of Toronto. For more information, see Planet Blue Coat: Mapping Global Censorship and Surveillance Tools, 15 November 2014. Available at https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

workers, especially for those are working with digital platforms including crowdsourcing tools and platforms. Humanitarian aid workers on the ground and other workers need to consider several risks. Network access and system continuity management are sensitive aspects to protect [11]. Trusted network access, with authentication of users and encryption might provide the required security. Some secured data backups would add new safeguards. The information gathering also needs security measures like a privacy-preserving information system and an authenticated broadcasting.

Other risks are due to personal information disclosure and location data management [11, 12]. For example, publicizing the details of victims, users, relief efforts etc. can put people associated with a particular crowdsourcing effort in danger. Easy procedures like mask up or forwarding, and more complicated ones like obfuscation and perturbation might be considered. Health information is sensitive data, and should thus be even more protected. Gender discrimination might also be present in crisis informatics. The rate of female staff in disaster management sections is only 5-10 per cent. Gender equality centres can help gender perspectives to be included in disaster management [13].

Risks related to retrieving and selection with crowdsourced data analytics

Accurate and relevant information can be selected by trained volunteers. But automated data collection and selection are increasingly used in crisis informatics. For instance, social networks data mining, user ranking, information automatic classification and sensors are examples of partial or complete automatic retrieving and selection.

Social network data mining risks

Social networks data mining can help extracting data from the public pages on emergency platforms. Security, access controls, and privacy are weak by design on most social networks

because their popularity and commercial value hinge upon their easy and open access to all Internet users [14]. As Social Media Platforms provide open and easy access, their users take many unconscious risks by publicly disseminating personal communication, personal information and images etc.

The quality of data depends heavily on data providers' profiles. Some 'general' crowd and subgroups of trusted volunteers provide data during crisis management work. There are potential risks for registered users as those volunteers have to provide personal information to create their profiles. Providing too much information while creating profiles is highly risky dangerous in terms of privacy, security and personal data protection. Thus, data mining after setting up a framework where the crowd i.e. digital volunteers verify data, respecting transparency, rights and open data policies and practices could be the solution [4].

However, by publicly announcing the 'trust' level of Social Networking Sites could reduce some risks mentioned earlier. Tech companies should develop tools with Privacy Enhancing Technologies (PET) integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as 'anonymous'. Private companies also should not illegally collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing platforms. Such type of illegal collection of personal data should be punishable by the Law [15].

User Ranking and content classification risks

Numbers of crowdsourcing platforms have ranking systems for their registered users, *i.e* trust in people first, then in data [**6**]. These platforms calculate users' activities like, the number of reports submitted or bookmarked, or successful or unsuccessful matches have been extracted and used to label the user as active or not, and as effective or not. To identify active users, users were ranked based on the number of their likes,

comments and posts. Active and effective users are thus preferred when taking into account the relevance and accuracy of data. On the other hand, high ranking volunteers were not always highly trustworthy participants in crowdsourcing crisis management activities. So, when they select and rank a crisis incident, they might do mistakes. Some participants can provide misleading information intentionally. In such type of cases, data is not cross checked among different sources and thus not validated. So, in such cases, a total accuracy is not possible.

In crowdsourcing crisis informatics, machine learning has been used to evaluate trustworthiness of Tweets automatically and within seconds. In Artificial Intelligence Disaster Response (AIDR), Twitter messages are classified by at least three volunteers. MicroMappers also combines volunteer filtering with machine learning on a "Text-Clicker" option. However, it has been noticed in some cases that ranking or scoring data using Machine Learning techniques is not hundred percent accurate at all time. To address the issues of content classification risks, crowdsourcing crisis coordinators should cross check crowdsourced data with other sources and finally, tally the analytics of data between digital volunteers and machines.

Risks associated with sensors

Valuable Information can be also crowdsourced by using mobile sensors. Geo-location information and other relevant data are sent to remote databases where machine learning takes place. However, wrong information gathering could also happen with sensors.

There are also some major privacy concerns due to the fact that sensors have the potential to detect levels of detail that were impossible earlier. As sensors have the ability to routinely gather data at a particular point or land mark, privacy suddenly becomes a major concern as sensors has potential to gather unwanted data as well. This privacy

dimension is informational and 'relates to those attributes, activities, or information that an individual may wish to conceal from others' [16]. Sensors may collect data on locations and habits of people and gathered data could be correlated with data coming from sensors from the real world. Thus, knowledge base virtual world contain pervasive information revealing individuals' habits, routines, or decisions [17]. Secondly, as gathering and manipulating information is a form of power in a global information economy [18]; enterprises can control data collections and knowledge bases. Thirdly, some oppressive governments also keep such data into their system to 'prevent' future crisis.

To deal risks associated with sensors, a safe-use framework should be developed and illegally collection of personal data should be made punishable by the law of the land [15].

Situational awareness risks

Generally, crisis management increasingly adds context information. It is called situation awareness and can be provided by individual volunteers and crisis communities (see 3.1), but also by situation awareness systems or risk estimation (see 3.2). The diversity of crisis situations which originated from different events and the variety of users and tools have in fact led crisis management organizations and crisis management coordinators to face specific risks covering different areas, including situational awareness, data visualization, (geo)visual analytics, visual representations, advanced (mobile) interfaces, communication technology and collaborative approach among different volunteer communities [19].

Situational awareness provided by volunteers and communities

Virtual volunteers usually employ group chat and Skype conversations and also some crisis informatics are now offering

management tools to these small support teams [20]. Volunteers provide geo-referenced information, like sensors would do, to contribute to crisis situational awareness. Accessing users' live video streaming, personal image updates, geo-location etc. can be effective for support teams in discovering the actual incident and selecting relevant data to allow emergency response teams improve their situational awareness [21], however, by accessing such activities of users' could infringe individual privacy. Real-time updates from users of location-based services, like microblogs, for instance create time-stamped and geo-located data using smart phones with GPS [22], also have a potential adverse perspective in terms of right to privacy and security. Some crowdsourcing tools force users to revel their geo-location information. For example, the crowd control LEEDIR (Large Emergency Event Digital Information Repository) demands access to GPS data and when images and video are uploaded using the LEEDIR application [23].

Sometimes, crisis responders are not highly trained with the use of emerging technologies. For example, in Spain, fire fighters use sensors during bush fires. They really cannot concentrate on sending temperature update using sensors as they concentrate in controlling bush fires. Sometimes, they left the sensor in one particular location and try to control bush fires in a different location. So, in such cases sensors are unable to send accurate information. In their research on collaboration exercises during rescue operation in Sweden, Berlin et. al (2014) identified, 'Organizations worked sequentially and in parallel but without common coordination' [24].

The issue of reporting information can be 'altered or restricted depending on the nature of the disaster in question, especially where there is lack of interagency communication' [28]. Real-time reporting of crisis is extremely useful but may cause another problem. For example, volunteers want to contribute but they work on ad-hoc basis. This happens because

of the lack of coordination. As all volunteers are not expert, they cannot follow coordinators' indication during crisis management work, while time management is one of the most important issues in any disaster. In most of the cases, crisis coordinators develop some predefined categories to identify the right information. However, predefined categories may risk excluding useful contents failing to capture contextual tone of the text [29]. Thus, lack of coordination is a major problem in implementing a successful disaster management process among inter-agencies involved [30].

Many disaster evaluation reports mention the issues like disconnects between relief organizations and local communities, a lack of information sharing between organizations, misalignment between needs and recovery actions, and sub-optimal decision making etc [32]. When disasters occur, organizations like the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) must quickly make decisions based on the most complete information of the situation they are able to obtain. They are responsible for organizing search and rescue operations, emergency food assistance, and similar tasks [33]. Normally, volunteer organisations are in charge of providing situational awareness during disasters. Organizations like the OCHA and other traditional organizations are able to submit a request and rely on the Digital Humanitarian Network to build a solution team with the relevant volunteer members within the volunteer communities.

Different information management officers (IMOs) and humanitarian affairs **o**fficers **(**HAOs**)** of the OCHA have different skill sets, but as a group, they are tasked with gathering data, liaising with various cluster leaders, communicating with volunteers, updating databases and common data repositories, and producing a variety of documents. In the immediate aftermath of a disaster, they often experience "ad-hoc craziness" brought on by a need to complete myriad tasks in a short period of time [34]. This core solution

support team decides on different aspects of crisis response works. However**,** current decision making support systems and frameworks do not appear to sufficiently handle dynamic decision-making supports in the contexts of any large-scale disaster situations [35].

Apart from this, there are concerns with the reliability and accuracy of crowdsourced data. In crowdsourcing, **'**while lower levels of abstraction (e.g., tweets with individual requests and specific local references) risk overwhelming the human reviewer, high levels of abstraction risk denying a role for human interpretation' [29]. As of now, there is no mechanism to demonstrate the accuracy of crowdsourced data after comparing with more 'traditional data' and also to document the efforts made on the evaluation and verification of the crowdsourced data. So far, just an example of a joint verification of data has been identified in Indonesia which was set up between Open Street Map, NGOs and the Government to build a stronger level of confidence [4]. Though, the organizations involved in crisis response work use social media to disseminate important information during crises, but government institutions and other established entities should use social media as a tool to disseminate information, so that users would rely on such trusted sources. Other risk is that even though numbers of organizations, donors, other partners work in a particular crisis, they do not take decisions together or work together on the same issue. If Ushahidi is working on such a crowdsourcing platform and OCHA/UNHCR has also developed a common platform - it is wastage of human resource, money and time. Such types of approaches by organizations bring less trust among citizens and individual crisis response platforms become more vulnerable and criminals can take the opportunities of this vulnerability.

Crowdfunding is one of the common functionalities for crisis management activities. Crisis victim communities can seek funds using crowdfunding channels and crowdfunding scams can take on many different ways. There have been

several incidents that have raised concerns about crowdfunding [36]. Apart from this, some information that humanitarians collect could be valuable to criminals. Account information for cash transfers is an obvious target, but other types of data may have value for insurance fraud, identify theft, or corruption [2].

On the other hand, collaboration between professional organizations is a major issue in disaster recovery. Duffy (Ed.) (2014) identified that the 'current state-of-the-art in technological support for recovery activities reflect the same variety, increasing the risk of misinformation and collaboration gaps. Each professional organization uses its' own support tools (e.g. EU platform GDACS; Global Disaster Alert Coordination System) which are not shared' and it has also been identified the reason is that due to competition for scarce funding. [32] To deal such decision making support risks, a general framework for context-aware multi-party coordination systems proposed by Way, and Yuan (2013) could be the answer which can be used to enhance the current understanding of emergency response systems as well as support situations requiring dynamic decision making for managing large complex crisis by multiple stakeholders [35].

Situational Awareness Services and risk estimation

In crowdsourced data, consent is very critical. As it has been mentioned earlier that when third party gather information about victims through VAVs or Satellites; or even try to gather reports something like, 'xyz' has been molested by the opposition group members etc. could be really problematic. Because of online nature of crowdsourced data and complex crisis environment, it is not possible all time to maintain the ethical principles of 'Not to Harm'. Larrauri (2014) describes, "Humanitarian actors at times argue that the imperative to save lives trumps the need for consent in certain situations and / or at certain levels of data aggregation". Recognising the importance of the argument, the author questions further, 'but how applicable is it to collecting data on civilian protection' as

'it is much harder to draw the line on what is life-threatening in a conflict context' [37]. Larrauri (2014) argues that 'there is significant trauma among local populations who have witnessed drone strikes that appeared to come from nowhere' as residents in conflict regions fear humanitarian UAVs as threatening military equipment. Humanitarian organisations need to address this issue speedily to have the best positive outcome of using UAVs in humanitarian crisis management.

Situational Awareness is a prerequisite for decision-making, and Decision support systems [38]. The advent of new technologies has changed the landscape of crowdsourcing crisis informatics considerably in recent years. The increasing trends of using different digital tools for humanitarian crisis management, crowdsourcing tool coordinators started giving more emphasis on smart technologies and frameworks in crisis management work. With readily available software platforms and tools such as online discussion platforms and news aggregators; different crowdsourcing platforms like GroupSourcing, Crisis Response Game, Use of Linked Open Data for crisis management, Digital Governance Framework for Crisis Management, Interactive 'Crowdsourcing Unheard Voices' Platform for Crisis Reporting, AIDR Use of satellite images by Amnesty International and use of Unmanned Aerial Vehicles (UAVs) [39, 40, 41, 42, 43, 44, 45, 46, 47, 48]. Though, organisations can now disseminate, acquire and analyse information more efficiently and comprehensively, there are some potential risks in using only machines for risk estimation as machines can do mistakes as well. On the other hand, well-skilled response team may still have better trust in their knowledge and experience than determine risks levels using only automatic tools. So, in decision-making for crisis governance work, the combination of machines and unskilled and semi-skilled operators could be risky. So, if humanitarian crisis response workers and others associated with humanitarian crisis work are not careful enough, their digital platforms including crowdsourcing platforms, 'their data

systems, particularly biometrics or other individual or household level registration tools, can be co-opted into becoming an extension of state surveillance, even after a crisis ends' [2].

However, there are some ways to be safe and protected while working in crisis period. Firstly, law enforcement agencies should not monitor crowdsourcing process for crisis governance to identify 'evidences' illegally in the suspicion of future terrorist attacks or conflicts (in man-made crisis). For counter-terrorism purpose governments could do so with prior judicial authorizations. Secondly, crisis response coordinators must collect and handle information containing personal details in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection. Thirdly, they should establish standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection. Fourthly, crisis governance coordinators must not use any digital tool that has potential risk of security breach and finally, they must develop guidelines for the crisis reporters and other users including journalists.

Decision support risks

The collection, analysis and interpretation of the earth's surface data for crisis management create some absolute risks. Like other aspects of crisis management activities, geomatics also has some general risks that include the security and privacy of a particular area and population of that area. For instance, earthquake, tsunamis and floods forecasting and modelling through remote sensing and geodetic data allows providing both long-term planning as well as short-term identification of most damaged areas [49, 50, 51]. Data mining and statistics on past events can also be useful for this purpose [52, 53].

Simulations are also increasingly used. For instance, modeling the movement of people until they escape from a hazard, *i.e.* activity recognition, can also be decision support

systems for disaster management. Thus mapping and evacuation planning under uncertainty, based on these simulations, are theoretically available [54, 55]. Fire detection has also being a preferred field for simulations. Since 2000 decision support systems help fire detection, reduce false alarms, offer fire data analysis and predict future fires [56]. Simulation is also suggested for floods management [57].

Rapid mapping[7] is another valuable data analytics technique for disaster management [58]. However, some features of rapid mapping can bring huge risks to the community, volunteers and victims of disasters. For instance, part of the map production is based on automatic affected population estimations or potential infrastructure damages evaluation. Obviously, this is only possible when there are areas with detailed reference datasets available, otherwise *ad-hoc* crowdsourced mapping would be necessary and that is not the ideal situation.

One of the exciting emerging techniques is being used during crisis response work is 'Sentiment Analysis'[8]. For instance, emotional behaviour simulations provide better assessments for emergency evacuations [59]. This natural language processing, text analysis and computational linguistics has the potential to provide wrong data analytics. Secondly, as this process uses some latest data mining techniques, there is huge chance for an individual to be exposed in public. So, this technique could violate right to privacy.

Along with security, privacy and data protection risks, the other risk of unlawful surveillance on decision support system also an important threat. The collection, analysis and interpretation of the earth's surface data for crisis management create some absolute risks. In terms of image analytics, it can

[7] On-demand and quick mapping (within hours or days) of geospatial information immediately after an emergency event. See more at http://bit.ly/1PyOvGs.

[8] Sentiment analysis is also known as opinion mining. It refers to the use of natural language processing, text analysis and computational linguistics to identify and extract subjective information in source materials.

also start with volunteer identification of objects and places, and then use data analytics or be available for expert response teams[9]. Here, the risk is, most of the cases volunteers do not gave proper consent to use images of a vital set up or information about an unknown individual and so far, there is very little safeguard to protect someone's data and privacy.

Crisis coordinators should use tools with PET[10] integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as 'anonymous'. On the other hand, crowdsourcing reporters in humanitarian crisis must ask for options to be 'anonymous'; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as users will be able to apply these options if needed.

Automatic decision and false positives

Use of automatic tools in crisis response work is extremely helpful if tools give the correct information. However, making decisions solely based on automatic crowdsourcing tools is highly risky. For example, forest fire spread predictions can successfully be assessed by using already gathered crowdsourced data through decision support systems. Such tools will not be effective if they fail to run quickly and on time. In different crisis response initiatives, real-time information is very helpful for making a decision. However, automatic decision systems lack the full trust.

To the best of our knowledge there is no concrete ruling of automatic decision and false positives. Nonetheless, some general principles issued from privacy and data protection are available. For instance, in one Opinion on Drones, the Article 29 of Data Protection Working Party offered some worthy recommendations [60]. Using drones for decision support system is a good example because they have visual recording

[9] For more, please visit http://www.tomnod.com
[10] Privacy Enhancing Technologies

and detection equipment. Several risks are highlighted in terms of safety, third party liability, privacy and "chilling effect", *i.e.* the legitimate exercise of civil liberties and rights. Some suggested privacy by design solutions are envisioned like processing the images by using blurring or other graphical effects, so as to avoid unnecessary identification of people. More interesting for our purpose are the recommendations for law enforcement reasons. Crisis management, likewise law enforcement, is an example of legitimate purpose. Even though, they should respect general privacy principles: necessity, proportionality, data minimisation, strict and restricted retention period. Also, there is a concrete principle directly related to automatic decision-making: the prohibition of automated enforcement of decisions solely based on machines. In other words, the data processed via automatic decision support systems should be further scrutinised by a human first response expert before any decisions adversely affecting an individual is made. Courts should also be able to review the decision-making process. Some internal and external supervisor should eventually check the compliant use of the system according to an *ad hoc* legal framework.

POSSIBLE SOLUTIONS

To sum up, the identified legal and ethical risks of crowdsourcing crisis informatics could be divided into three stages. The stages are 1) Retrieval and Selection; 2) Situational Awareness; and 3) Decision Support System. Possible solutions for all stages will be mentioned in a form of tables in the next page. No explanatory text will be given about these solutions as an extensive explanation will require more pages. An extensive explanation will be given in an upcoming research work.

Retrieval and Selection (RS)

Retrieval and Selection by Volunteers	
Risks	Possible Solutions
Security breaks: cyber-attacks, nuisance attacks Mass surveillance	Trusted network access, authentication, encryption, data backups, privacy-preserving information systems authentication broadcasting
Quality and accuracy of data	Filtering, cross-checking, verification by the crowd
Personal Information Disclosure, location management, sensitive data	Mask up, forwarding, obfuscation, perturbation, Additional safeguards for sensitive data.
RS by Data Analysis	
Risks	Possible Solutions
Profiling with data mining	Privacy preserving data mining Privacy Enhancing Technologies (PET)
Geolocation using sensors	PET for geolocation
User ranking and content classification	Cross-checking

Situational Awareness (SA)

Risks	Possible Solutions
SA by Volunteers	
Geo-referenced information	PET for geolocation
Lack of coordination between experts and volunteers	Solution Support Teams
Lack of collaboration between agencies	Context-aware multi-party coordination systems
SA by Data Analytics	
Non-acceptance of SA services by users	Purpose limitation (only for disaster management)
Information collection and storage	PET

Decision Support Systems (DSS)

Risks	Possible Solutions
Reliability	Cross-Checking
Decision adversely affecting humans solely based on	First response team monitoring and cross-checking

automatic DSS	
Traceability of the automatic decision	Logs and internal and external supervision

CONCLUSION AND FUTURE WORKS

As numbers of crowdsourcing crisis informatics risks have been identified in this paper, the future work would be to identify the possible solutions of those risks. Based on different scenarios, it has been identified that trusted network access, authentication, encryption, data backups, privacy-preserving information systems, authentication broadcasting, filtering, cross-checking, verification by the crowd, mask up, forwarding, obfuscation, perturbation, additional safeguards for sensitive data, privacy preserving data mining, Privacy Enhancing Technologies (PET), PET for geolocation, Context-aware multi-party coordination systems, proper Solution Support Teams, Purpose limitation (only for disaster management), first response team monitoring and cross-checking etc are needed to solve present risks associated with crowdsourcing crisis management.

The future work would be to develop general framework for crowdsourcing crisis informatics comprising with potential legal, ethical and technical solutions for the next generation crisis response work.

ACKNOWLEDGMENTS

This paper is supported through a Doctoral Fellowship LAST-JD PHD program (www.last-jd.eu). The author would like to thank his supervisor Dr. Antoni Roig (IDT-UAB) for his support, guidance and feedback on this manuscript.

REFERENCES

[1] United Nations, 2015. Preamble of the Sendai Framework for Disaster Risk Reduction 2015-2030, (A/CONF.224/L.2) the

final outcomes of the Third United Nations World Conference on Disaster Risk held in March 2015.
[2] OCHA, 2014. Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies, Occasional Policy Paper, OCHA Policy and Studies Series 2014.
[3] Gao, H., Wang, X.. Barbier, G. and Liu, H (2011). Promoting Coordination for Disaster Relief– From Crowdsourcing to Coordination in J. Salerno et al. (Eds.): SBP 2011, LNCS 6589, pp. 197–204, 2011. Springer-Verlag Berlin Heidelberg 2011.
[4] United Nations, 2013. Report on the International Expert Meeting on Crowdsource Mapping for Disaster Risk Management and Emergency Response carried out in the framework of the United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) Report No. A/AC.105/C.1/2013/CRP.5 presented by the Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee at Fiftieth Session in Vienna during 11-22 February 2013.
[5] Gao, H., Barbier, G., Goolsby, R. (2011). Harnessing the crowdsourcing power of social media for disaster relief. IEEE Intelligent Systems 26(3), 10–14 (2011).
[6] Tapia, A. H., and Moore, K., Good Enough is Good Enough: Overcoming Disaster Response Organizations' Slow Social Media Data Adoption, Computer Supported Cooperative Work (CSCW) (2014) 23:483–512.
[7] Gilman, D. 2014. Cyber-Warfare and Humanitarian Space, in Llorente, R. V. and Wall, I. (eds.) Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF).
[8] Gilman, D. 2014. Cyber-Warfare and Humanitarian Space, in Llorente, R. V. and Wall, I. (eds.) Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF).

[9] Byrne, R. 2014. Trends in Intelligence Gathering by Governments, in Llorente, R. V. and Wall, I. (eds.) Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF).
[10] Fisher, M. 2013. Syria's Pro-Assad Hackers Infiltrate Human Rights Watch Web Site and Twitter Feed, The Washington Post, 17 March, 2013. Available at http://wapo.st/1xSz3T7
[11] Kiyomoto, S., Fukushima, K., and Miyake, Y., Security issues on IT systems during disasters: a survey, J Ambient Intell Human Comput (2014) 5:173–185.
[12] Wu,S.-Y., Wang, M.-H., and Chen, K.-T., Privacy Crisis due to Crisis Response on the Web, 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST.
[13] Saito, Y., Progress or repetition? Gender perspectives in disaster management in Japan, Disaster Prevention and Management Vol. 23 No. 2, 2014 pp. 98-111
[14] Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers, 22(5), 428-438.
[15] Halder, B. 2014. Crowdsourcing collection of data for crisis governance in the post-2015 world: potential offers and crucial challenges. In Proceeding ICEGOV '14 Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance. ACM New York, NY, USA ©2014.
[16] Slonecker, E. T., Shaw, D. M., and Lillesand, T. M.: Emerging Legal and Ethical Issues in Advanced Remote Sensing Technology. Photogrammetric Engineering & Remote Sensing, Vol. 64, No. 6, June 1998, pp. 589-595.
[17] Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011). A survey on privacy in mobile participatory sensing applications. Journal of Systems and Software, 84(11), 1928–1946.

[18] Lievrouw, L. A., & Farb, S. E. (2003). Information and social equity. In Cronin, B. & Shaw, D. (Eds.), Annual review of information science and technology, Volume 37 (pp. 499–540).
[19] Ginige, A., Paolino, L., Romano, M., Sebillo, M., Tortora, G., & Vitiello, G. (2014). Information Sharing Among Disaster Responders - An Interactive Spreadsheet-Based Collaboration Approach. Computer Supported Cooperative Work (CSCW) (2014) 23:547–583. DOI 10.1007/s10606-014-9207-0.
[20] Poblet, M. (ed.), (2011) Mobile Technologies for Conflict Management: Online Dispute Resolution, Governance, Participation, Law, Governance and Technology Series 2, DOI 10.1007/978-94-007-1384-0_4, © Springer Science+Business Media B.V. 2011.
[21] Ajmar, A.,Boccardo, P., Disabato, F. and Tonolo, F.G. (2015). Mapping: geomatics role and research opportunities, Rend. Fis. Acc. Lincei, Springerlink.com.
[22] Chae J., Thomb, D., Jang Y., Kim S.Y., Ertl, T. And Ebert D.,S., Public behavior response analysis in disaster events utilizing visual analytics of microblog data, Computers and Graphics, 38, 51-60 (2014).
[23] Cushing, T., 2014. Los Angeles Law Enforcement Looking To Crowdsource Surveillance, (Mis)Uses of Technology. Published at http://bit.ly/S4d6wE. Accessed on 12/05/14
[24] Berlin, J. M. and Carlstro, E. D.: (2014). Collaboration Exercises—The Lack of Collaborative Benefits. International Journal of Disaster Risk Science (2014) 5:192–205 www.ijdrs.com. DOI 10.1007/s13753-014-0025-2.
[25] Meier, P. (2011). OpenStreetMap's New Micro-Tasking Platform for Satellite Imagery Tracing. Available at http://bit.ly/1Jagm31 Accessed on 01/06/2015.
[26] Meier, P. (2013). Tag Tweets to Support Typhoon Relief Efforts in Philippines! Accessed on 02/06/2015 and available at http://bit.ly/1OpRfIr.
[27] Meier, P. (2013). Live Crisis Map of Disaster Damage Reported on Social Media. Accesed on 02/06/2015 and available at http://bit.ly/1SpNxCm

[28] Meier, P. (2013). Live Crisis Map of Disaster Damage Reported on Social Media. Accesed on 02/06/2015 and available at http://bit.ly/1RtEnos

[29] Purohit, H., Hampton, A., Bhatt, S., Shalin, V.L., Sheth, A. P. & Flach, J. M. (2014). Identifying Seekers and Suppliers in Social Media Communities to Support Crisis Coordination. Computer Supported Cooperative Work (CSCW) (2014) 23:513–545. DOI 10.1007/s10606-014-9209-y.

[30] Sweta, L.O. 2014.: Early Warning Systems and Disaster Management using Mobile Crowdsourcing . International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 . Volume 3 Issue 4, April 2014.

[31] Meier, P., 2013. Data Protection Protocols for Crisis Mapping available at http://bit.ly/1u11vfN

[32] V.G. Duffy (Ed.) (DHM 2014). HCI Challenges for Community-Based Disaster Recovery. LNCS 8529, pp. 637–648, 2014. Springer International Publishing Switzerland 2014.

[33] L.M. Aiello and D. McFarland (Eds.): Integrating Social Media Communications into the Rapid Assessment of Sudden Onset Disasters. SocInfo 2014, LNCS 8851, pp. 444–461, 2014. Springer International Publishing Switzerland 2014.

[34] Verity, A., Mackinnon, K., Link, Y.: OCHA information management guidance for sudden onset emergencies. Tech. rep., UN OCHA (Feb 2014).

[35] Way, S., Yuan, Y. (2013). Transitioning From Dynamic Decision Support to Context-Aware Multi-Party Coordination: A Case for Emergency Response. Group Decis Negot (2014) 23:649–672. DOI 10.1007/s10726-013-9365-3.

[36] Patterson, E. 2013. Crowdfunding Sites Grapple with Fraud, Better Business Bureau. Available at http://www.bbb.org/blog/2013/06/crowdfunding-sites-grapple-with-fraud/ Accessed on 11/11/2014

[37] Larrauri, H. P. 2014. Drones, ethics and conflict. Accessed on 10/11/2014 andavailable at http://bit.ly/1qUwRER

[38] Naderpour, M. and Guangquan Zhang, J.L., 2014: An intelligent situation awareness support system for safety-

critical environments, Decision Support Systems, 59, 325-340 (2014).
[39] Gao, H., Wang, X.. Barbier, G. and Liu, H (2011). Promoting Coordination for Disaster Relief– From Crowdsourcing to Coordination in J. Salerno et al. (Eds.): SBP 2011, LNCS 6589, pp. 197–204, 2011. Springer-Verlag Berlin Heidelberg 2011.
[40] Abbasil, M., Kumar, S., Filho, A, and Liu, H. (2012). Lessons Learned in Using Social Media for Disaster Relief - ASU Crisis Response Game in S.J. Yang, A.M. Greenberg, and M. Endsley (Eds.): SBP 2012, LNCS 7227, pp. 282–289, 2012. Springer-Verlag Berlin Heidelberg 2012.
[41] Ortmann, J., Limbu, M., Wang, D. and Kauppinen, T. (2011). Crowdsourcing Linked Open Data for Disaster Management, Institute for Geoinformatics, University of Muenster, Germany.
[42] Halder, B. 2013. SMS2FAX: A Tool to Enhance Public Service in Emergency Situation. International Journal of Computer and Communication Technology, ISSN (PRINT): 0975 - 7449, Volume-4, Issue-3, 2013. p 16-21.
[43] Halder, B. 2014. CrowdCriMa - a complete Next Generation Crowsourced Crisis Management Platform. Accessed on 07/06/2015 and available at http://bit.ly/1WjOyuW
[44] Imran, M., Castillo, C., Lucas, J., Meier, P. and Vieweg, S. (2014). AIDR: Artificial Intelligence for Disaster Response presented at WWW'14 Companion, April 7–11, 2014, Seoul, Korea. ACM 978-1-4503-2745-9/14/04. http://dx.doi.org/10.1145/2567948.2577034.
[45] Amnesty International, (2013). Aleppo satellite images show devastation, mass displacement one year on. Accessed on 08/10/2014 and available at http://bit.ly/1PjlRJ3
[46] Meier, P. (2014). On UAVs for Peacebuilding and Conflict Prevention. Available at http://bit.ly/1t6ueAD and Accessed on 10/11/2014
[47] Robinson. A. C. (2014). Emerging Theme: UAVs and DIY Drones, Planning GIS for Emergency Management. Penn State

University, 2014. Accessed on 08/10/2014. Available at https://www.e-education.psu.edu/geog588/l2_p5.html
[48] Ezequiel, C A F., Cua, M., Libatique, N. C., Tangonan, G. L., Alampay, R., Labuguen, R. T., Favila, C. M., Honrado, J.L.E., Ca˜nos, V., Devaney, C., Loreto, A. B., Bacusmo, J. and Palma, B. (2014). UAV Aerial Imaging Applications for Post-Disaster Assessment, Environmental Management and Infrastructure Development. 2014 International Conference on Unmanned Aircraft Systems (ICUAS). May 27-30, 2014. Orlando, FL, USA. p. 274-283.
[49] Glasscoe, M.T., Wang,J., Pierce, M.E., Yoder, M.R., Parker, W., Burl, M. C., Stough, T.M., Granat, R.A., Donnelan, A., Rundle, J.B., Ma, Y., Bawden, G. W., and Yuen, K., E-DECIDER: Using Earth Science Data and Modeling Tools to Develop Decision Support for Earthquake Disaster Response, Pure Appl. Geophys., April 2014.
[50] Susaki, J., Region-based automatic mapping of tsunami-damaged buildings using multi-temporal aerial images, Nat Hazards (2015) 76:397–420.
[51] Mancini, F., Capra, A., Castagnetti,C., Ceppi, C., Bertacchini, E., and Rivola, R., Contribution of Geomatics Engineering and VGI Within the Landslide Risk Assessment Procedures, O. Gervasi et al. (Eds.): ICCSA 2015, Part II, LNCS 9156, pp. 635–647, 2015.
[52] Radianti, J., Granmo, O.C, Sarshar, P., Goodwin, M., Dugdale, J, Gonzalez, J.J., A spatio-temporal probabilistic model of hazard- and crowd dynamics for evacuation planning in disasters, Appl Intell (2015) 42:3–23.
[53] Tehrany, M.S., Lee, M.J., Pradhan, B., Jebur, M.N., Lee, S., Flood susceptibility mapping using integrated bivariate and multivariate statistical models, Environ Earth Sci (2014) 72:4001–4015.
[54] Chou, J.S. and Lee, C.M., Integrating the geographic information system and predictive data mining techniques to model effects of compound disasters in Taipei, Nat Hazards (2014) 70:1385–1415.

[55] Sadiq, F.I., Selamat, A. and Ibrahim, R., Human Activity Recognition Prediction for Crowd Disaster Mitigation, N.T. Nguyen et al. (Eds.): ACIIDS 2015, Part I, LNAI 9011, pp. 200–210, 2015.
[56] Mahdipour, E. and Dadkhah, C., Automatic fire detection based on soft computing techniques: review from 2000 to 2010, Artif Intell Rev (2014) 42:895–934.
[57] Konev, A., Waser, J.,Sadransky,B., Cornel, D., Perdigão, R.A.P., Horváth, Z., and Gröller, M.E., Run Watchers: Automatic Simulation-Based Decision Support in Flood Management, IEEE Transactions on Visualization and Computer Graphics, Vol. 20, no. 12, December 2014.
[58] Foresti, G.,L., Farinosi, M. and Vernier, M., Situational awareness in smart environments: socio-mobile and sensor data fusion for emergency response to disasters, J Ambient Intell Human Comput, 6:239–257 (2015).
[59] Kefalas, P., Sakellariou,I., Basakos, D. and Stamatopoulou, I, A Formal Approach to Model Emotional Agents Behaviour in Disaster Management Situations, A. Likas, K. Blekas, and D. Kalles (Eds.): SETN 2014, LNAI 8445, pp. 237–250, 2014.
[60] Opinion 01/2015 of the Article 29 data Protection Working Party on Privacy and Data Protection Issues relating to the utilisation of Drones, 16 June 2015 (01673/15/EN, WP 231).
[61] Ferzan, K.K., Preventive Justice and the Presumption of Innocence, Crim Law and Philos (2014) 8:505–525.
[62] Cole, D., The Difference Prevention Makes: Regulating Preventive Justice, Crim Law and Philos, March 2014.