zif Center for International Peace Operations

# 100 Voices on Technology & Peace Operations

Enhancing situational awareness and mission protection through digital technologies

# Crisis informatics insights for peace operations

**18 December 2020** | Jasmin Haunschild, Prof. Dr. Christian Reuter, Dr. Marc André Kaufhold

Crisis Informatics – a field combining computing and social science to make visible and support the creative ways in which humans use information and communication technology (ICT) to respond to crises – has made many contributions in the areas of rapid crisis management. Interactive technologies such as social media platforms or emergency apps connect and empower individuals, first responders and volunteers. In a previously published review, we show that for almost 20 years, studies have analyzed ICT in natural and man-made disasters, revealing that ICT enable new modes of communication among authorities and citizens. In this contribution, we relate crisis informatics insights concerning the involvement of citizens to peace operations and community engagement.

Two circumstances make insights from Crisis informatics particularly applicable to peace operations: on the one hand, peace operations often have to deal with crises related to security incidents or natural disasters. A report by the Overseas Development Institute shows that 58% of disaster deaths and 34% of people affected by disasters have occurred in countries that appear in the top 30 of the Fragile States Index.

On the other hand, peace operations have to perform under conditions of limited access to infrastructures which are also typical in crisis situations. In the following, we also discuss differences regarding access to the internet and the availability of technologies as well as different political constellations that affect authority in crises.

## TAKING ADVANTAGE OF ALL COMMUNICATION DIRECTIONS

Another report by the Overseas Development Institute finds that "state-driven DRR [disaster risk reduction] policies and practices are simply not relevant and/or appropriate for the complex, informal and uncertain local risk realities in which the vast majority of poor people on the planet live and work. Alternative entry points are required."

Developing tools and practices that foster the involvement of citizens in such contexts could be such an entry point. Crisis informatics shows that individual and community engagement in crises is fostered through ICTs and that citizens, volunteers and emergent groups communicate amongst

themselves as well as with authorities, both as senders and receivers. Figure 1 shows how crisis information can thus be conceptualized as flowing from authorities to authorities (A2A); from authorities to citizens (A2C), as well as from citizens to authorities (C2A) and from citizens to citizens (C2C).

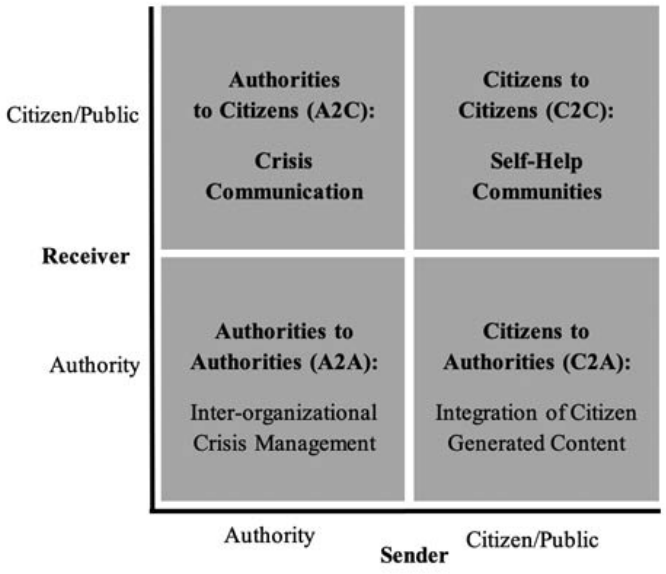


**Figure 1**: Crisis Communication Matrix

In the context of peace operations, authorities could mean a number of actors, depending on who holds de-facto authority in a local setting. This could be the mission, the host government, district or local level authorities and non-state (armed) groups that fulfill a quasi-state function. Citizens in peace operations are individuals, communities and also civil society organizations and informal organizations tasked with emergency response.

**Citizens to Citizens:** In crises, citizens communicate amongst themselves to grapple with what has occurred and to offer information and support. Types of online behavior in the context of crises that have been identified are helping, being anxious, returning, supporting, mourning and exploiting. Social media platforms can serve to coordinate volunteers in response to a crisis. Specific crisis management tools for social media have been developed that enable coordination, e.g. allowing to search and respond to requests and offers across multiple groups and platforms at the same time.

However, situational awareness is limited by biased data due to uneven distribution of internet access, especially in rural areas and along a gender divide. In Somalia, for example, the internet penetration, as of 2015, was roughly 1.7 percent of the population, while the average penetration across the rest of Africa is 28.6 percent. Another example is the penetration rate of Facebook accounts in 2017 which was at 37% in Syria, at 56% in Lebanon and at 8% in Somalia. Of those accounts, 82.8% were male in Somalia and 55.1% in Lebanon. In many countries with peace

operations a digitally active diaspora exists that can help with translations and mobilization of relief.

**Citizens to Authorities**: Instead of using unfocused citizen-generated content, citizens can also be called on by agencies and emergency management to provide specific information or to report specific situations, e.g. through warning apps or short messaging services (SMS). Often, citizens wish to be involved in security related tasks, e.g. contributing witness reports or supporting the search for missing persons. However, experiences in peacekeeping environments suggest that this is only suitable for situations where citizen informants do not run the risk of becoming targets of violent groups. Instead of providing specific emergency tools, the use of general-purpose tools such as messaging apps can increase adoption and avoid endangering citizens. This is especially important where citizens have to fear reprisal by armed non-state groups for appearing too close to the government, who may also be providing emergency assistance.

**Authorities to Citizens**: While traditional media such as radio and TV, as well as low-tech warning systems such as sirens are still important for spreading critical emergency information, agencies can also use general-purpose tools such as social media and chat messengers to alert citizens and provide recommendations. Built-for purpose tools such as warning apps can offer more options, such as location-specific information, offline instructions and information for emergency preparation. This may be easier for safety aspects such as extreme weather, sending recommendations for how to react or how to prepare for extreme events, or sending instructions about evacuations. ICT applications for security aspects such as warnings about violent clashes in peace operations should consider the potential for abuse by government agencies to increase perceived insecurity and potentially triggering displacement. Peace operations should consider offering their own tools to ensure neutrality and credibility of the warnings.

**Authorities to Authorities**: So far, digital and network-enabled communication on an inter-organizational level is focused on real-time and geo-tagged reporting and enables the on-the-ground staff to receive a better understanding of their operations environment, adding to daily reports. Due to privacy, confidentiality and impartiality/neutrality aspects, social media is often of only limited use in the context of peace operations. Since state structures are typically fragile in the context of peace operations, the following focuses on crisis ICT use that fosters citizen and community engagement.

## COORDINATING CITIZENS' ACTIVITIES IN EMERGENCIES

Citizens and authorities can take on a range of roles during emergencies and crisis situations, as illustrated in Figure 2. Out of citizen crisis communication and coordination specific offline and virtual roles emerge, such as digital volunteers that are for example involved in crisis mapping, as well as repeaters and retweeters of important information on social media. Connecting the virtual and real realm helps to identify needs that are reported only and moderated on social media groups in an effort to match needs and offers.

Authorities, while tasked with incident management and classic emergency response, including

coordinating volunteers on the ground, should also provide channels and personnel to liaise with the virtual and technical communities. This virtual component of authority response can be fulfilled by Virtual Operations Support Teams (VOST), that coordinate virtual and real-world activities. VOSTs can be either officials or trusted volunteers who inform on-the-ground operations about social media activity and coordinate virtual volunteers in a manner that supports on-the-ground activities, reporting to mission or state-run incident management. Virtual and technical communities are volunteer groups who act in the virtual realm e.g. reporting from the ground, moderating social media groups or coordinating help. Particularly where internet users are clustered in cities and in the diaspora, investing in roles that coordinate that remote activity of virtual and technical communities, which are often involved in online campaigning, database management or geo-referencing, is recommended.

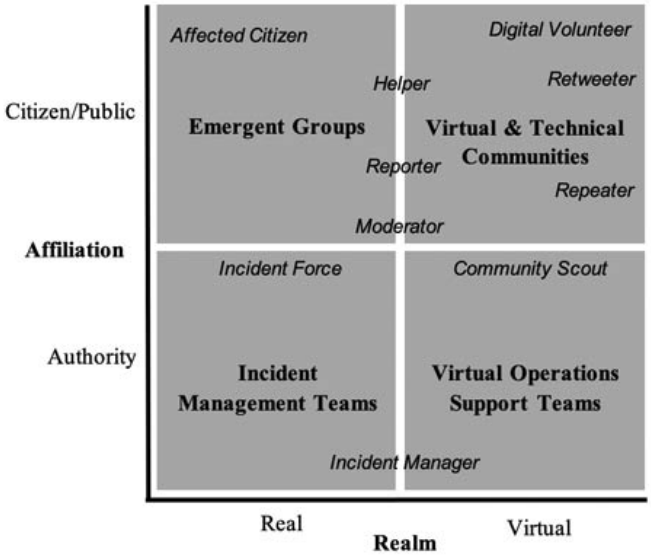


**Figure 2**: Role Typology Matrix

## REQUIREMENTS FOR CITIZEN INVOLVEMENT IN CRISIS COMMUNICATION

In order to successfully involve citizens in digital crisis communication two main factors need to be considered in each case: Access to the internet and to a mobile device, on the one hand, and local risk culture and the willingness of citizens to engage through digital tools, on the other. Data from the World Bank shows that both the internet and the mobile phone usage are rising but that they also differ between countries with UN peace operations and within fragile countries. The fact that mobile phones are widely available can help in countries with low internet use, where online warnings can be passed on via SMS or calls.

# 100 Voices on Technology & Peace Operations

**Figure 3**: Individuals using the Internet (% of population)
Source: World Development Indicators

**Figure 4**: Mobile cellular subscriptions (per 100 people)
Source: World Development Indicators

The data shows that internet use differs starkly between countries, making social media analysis less feasible in some countries, while it is wide-spread in others, particularly outside of Africa and in urban centres. However, even where internet usage is low, mobile phones are relatively wide-spread, suggesting that low-tech and offline interventions are promising.

While reliable data are difficult to obtain, some data collections also suggest that internet and mobile device use vary greatly, suggesting 10% of internet and social media user and 48% of mobile connections in Somalia in 2020, 24% internet, 8.5% social media use and 108% mobile connections in Mali, 35% social media and 83% mobile connections in Syria, to name but a few examples.

While social media use is thus low in Somalia, a study of Somali students at a Malaysian university suggests that diaspora communities are using social media more strongly. The study revealed three-quarters of students used social media in 2012, including to raise awareness about the famine. The public Facebook group "Somali Students on Facebook" has almost 21.000 members. This shows that even where internet and social media use are low, engaging a diaspora in times of crises may be helpful for disaster managers and UN missions.

## RISK CULTURES INFLUENCE ATTITUDES AND ONLINE BEHAVIOR

Another relevant aspect is the local risk culture. While a concept developed in an analysis of Western states, the insights show that attitudes and expectations in a crisis also influence online behaviour and attitudes towards crisis tools. Countries might have a state-oriented risk culture or an individualistic risk culture or a fatalistic risk culture, where citizens turn to and rely on different channels and tools of communication in accordance with the dominant risk culture.

Countries that can be described as having a state-oriented risk culture, where trust in state authorities is high and authorities are regarded as responsible for keeping citizens safe, and where crises are regarded as influenced by humans and the environment, citizens rely more on official channels and mass media than on social media.

In individualistic risk cultures, citizens feel more individually responsible for their safety and have relatively good understanding of coping mechanisms. Individuals in these cultures appear readier to use emergency warning apps. Insights suggest that citizens particularly rely on social media in places where they perceive a need for improvement of crisis management.

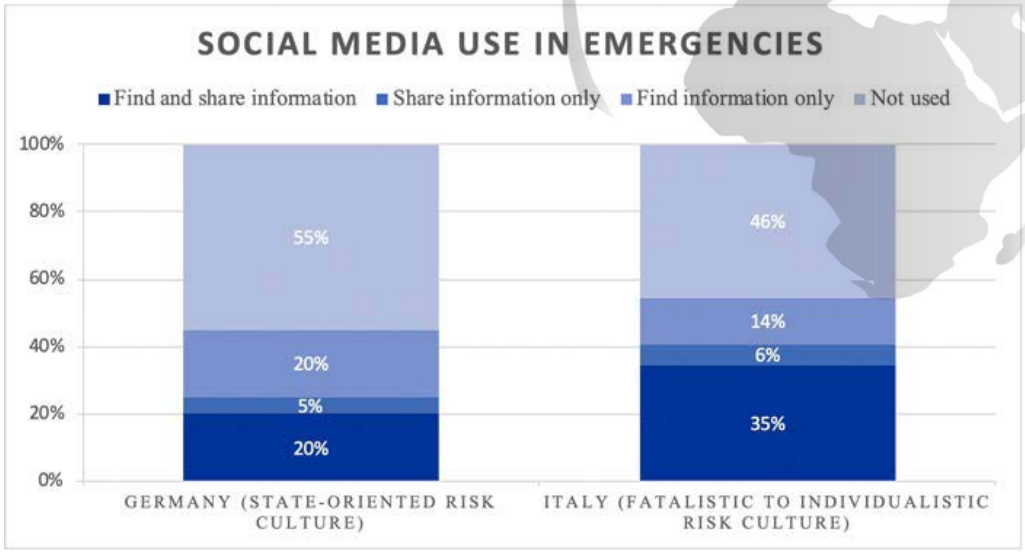


**Figure 5**: Depiction of social media use in a state-oriented country (Germany), in a fatalistic evolving to individualistic one (Italy).

A fatalistic risk culture perceives hazards as unpredictable and unavoidable, showing low trust in authorities due to prior inefficacy and in mass media which is perceived as subjective. Individuals have low confidence in their problem-solving potentials. While they still generally expect the state to act during emergencies, they are less likely to take state communications such as warnings seriously and to use technical tools for individual measures.

## CONCLUSION: USING INFORMATION AND COMMUNICATION TECHNOLOGIES TO INVOLVE CITIZENS IN EMERGENCIES

More than fifteen years of research in crisis informatics show that information and communication technologies offer opportunities for involving citizens in crisis situations, by

1. reaching citizens faster through social media, warning apps, SMS or recently also messaging channels;

2. informing intervention through citizen-generated content or two-way communication, e.g. using built-for-purpose apps; and

3. fostering self-help and self-coordination of volunteers and affected citizens.

Clearly, the use of information and communication technologies also threatens to disadvantage those who do not have mobile internet access. It should therefore be considered as an additional

avenue for reaching a limited group of (particularly young and urban) citizens, e.g. for emergency alerting or sharing of information about crisis risk reduction through social media. crisis apps or messengers. Authorities (be they from the peace operation or governmental) should also consider and connect with digital emergent groups that may be relevant for coordinating aid and relief or contributing to situational awareness. Research also shows that citizens are often keen to spread emergency information, facilitating outreach beyond internet users.

As a result, different groups of stakeholders should be considered when including social media in crisis strategies:

1. Non-users of the internet to whom information may be forwarded through low-technology channels and who may profit from volunteers' work coordinated online or whose contribution may be communicated by others into the online realm.

2. Local populations with internet access who can be informed though social media, spread information or self-coordinate and who can use tools such as warning apps for crisis alerts and information on crisis prevention.

3. Non-affected people who, in a crisis, can contribute remotely, including in diasporas..

The different roles engendered by social media include different challenges that can be addressed with the help of different tools. While false information can be a challenge, it is often corrected by other users, by moderators or official channels, even with the help of technology to rank high-trust information, or by presenting indicators of fake news to users. Tools such as XHELP enable moderators on social media to coordinate helpers more efficiently.

Within peace operations as well as outside of them, trust is a central aspect for involving citizens in crisis response. It is important for warnings to be believed and for recommendations to be followed. In addition to this top-town exchange, trust can be fostered through the integration and support of self-help activities. Peace operations should therefore include trained virtual operations support teams that can identify, support and integrate local self-help and external support activities that take place on social media.

## ABOUT THE AUTHORS

Advances in science and technology, especially in information technology (IT), play a crucial role in the context of peace and security. The research group Science and Technology for Peace and Security (PEASEC) led by Prof. Dr. Christian Reuter in the Department of Computer Science at Technische Universität Darmstadt deals with the significance of IT for safety, security and peace. This includes both empirical research on the perception and use, as well as technical research on the design of novel technologies and applications. Jasmin Haunschild and Dr. Marc André Kaufhold research information and communication technologies in the context auf crises and insecurity.