Repairing Human Infrastructure in a War Zone

Gloria Mark
University of California, Irvine
gmark@uci.edu

Ban Al-Ani
University of California, Irvine
balani@ics.uci.edu

Bryan Semaan
University of California, Irvine
bsemaan@uci.edu

ABSTRACT

People depend on human infrastructure for a range of activities in their daily lives, such as work and socializing. In this paper we consider three different intertwined types of infrastructures of a society that may be affected in crisis situations: the physical, technological, and human infrastructures. We argue that when the human infrastructure is damaged, e.g. in a natural catastrophe or war, then people can switch reliance to the technological infrastructure to be resilient. We conducted an empirical study of 85 people who lived in war zones during the 2006 Israeli-Lebanon war and the ongoing Gulf war in Iraq. In this paper, we report how information technology is used by our informants in new ways in their attempt to maintain social relationships and continue working. Our informants also used technology to help navigate safe routes for travel and for psychological support. We discuss implications of our results for disaster research.

Keywords

Human infrastructure, collaboration, war, Internet, information technology

INTRODUCTION

A number of recent studies have brought attention to how information technology (IT) is used to support people in communication and coordination in crisis situations. These studies have departed from focusing on the role of centralized information broadcast through official channels to show instead how residents collectively act to disseminate critical information about the event. Case studies have shown, for example, how people participated to construct lists of victims in the Virginia Tech shootings (Vieweg et al., 2008), to use the web as an information repository during Hurricane Katrina (Palen and Liu, 2008), and to use social media to spread locally relevant information during the Southern California wildfires (Shklovsky et al., 2008).

In this paper we continue this focus on IT use in disrupted environments but shift the attention from information dissemination to focus on how IT is used as a resource to enable people to act. To do this we look at the role of infrastructure in disrupted environments. Infrastructure is defined as: "*the underlying foundation or basic framework (as of a system or organization)*" (Merriam-Webster, 2008). A society relies on infrastructure to function. Systems such as power grids or highways are part of infrastructure. Institutions such as hospitals or government offices are also infrastructure. We consider three different intertwined types of infrastructures of a society that may be affected in crisis situations: the physical, technological, and human. Physical infrastructure refers to the physical foundation of roads, buildings, bridges, sewers, water pipes, etc. By technological infrastructure, we primarily refer to computing infrastructure supporting communication and the sharing of information, consisting of routers, servers, computers, wireless connectivity, landlines, satellites, cell phones, television, and so on.

The notion of human infrastructure has received perhaps the least attention in research studies. We consider the human infrastructure to be the underlying foundation of a social system constituted by the pattern of relationships of people, through various networks and social arrangements. Residents in a society depend on human infrastructure for a range of activities in their daily lives, i.e. for work, socializing, education, health care, entertainment, and so on. The human infrastructure can be comprised of family members and friends, work colleagues, neighbors, people in the health care profession, shop and restaurant owners, taxi drivers, policemen, administrators, etc. Human infrastructure differs from the concept of social network in that it is far broader. For example, an administrative assistant in one's workplace may not be part of one's social network but this person is part of the human infrastructure, as he or she supports the functioning of the workplace by delivering messages, financial or travel information, scheduling meetings, and conducting other support activities. Similarly, a pharmacist, nurse, or doctor may not be members in one's social network but they support people in

maintaining and restoring health and getting medications. Without an intact human infrastructure people cannot carry out familiar routines.

Commonly though, relationships concerning infrastructure are not so clearly delineated. For example, communication among people involves all three infrastructures. People may use cell phones or email to communicate or they may travel on roads using cars or public transport to meet each other. Depending on conditions people may also change how they use and rely on infrastructure. For example, if in a war zone one road is destroyed, then in order to meet people might take an alternative road that is still intact. Alternatively, people may cease travel and instead use email or telephone to communicate with others without physically meeting.

Star and Ruhleder (1996) describe how human infrastructure is interwoven with technological and physical infrastructures. They describe how infrastructure is generally invisible (such as plumbing) until it breaks down in which case it then becomes visible. When the computer network goes down then suddenly people become aware of it. Especially in a war environment, when roads are not passable or when electricity is not available then the physical and technological infrastructures becomes highly visible. As infrastructures are intertwined, changes in the use of one infrastructure may also affect how other infrastructures are used. For example, when new technology is adopted, new conventions of practice must be developed which in turn can change collaborative relationships. Whereas physical infrastructure is slow to change (e.g. a new building requires time for design and construction) human infrastructure is highly dynamic (Lee et al., 2006). In other words, people can readily reconfigure social arrangements, and consequently communication and coordination.

It is not any single group or social network that exists as human infrastructure, but rather the holistic constellation of networks, groups, relationships and patterns of communication that exists as a framework for any society or social unit. When human infrastructure is affected at a micro level (e.g. when an individual cannot meet face-to-face with colleagues and the individual must find new ways to communicate remotely with colleagues), then this new communication pattern can have a ripple effect on practices at a more macro group or even societal level.

We argue that when one infrastructure is damaged, as in a natural catastrophe or war, then people can switch reliance to a different infrastructure to be resilient, i.e. to continue to carry out their activities (Kendra and Wachtendorf, 2003). For example, if during a catastrophe people who one usually depends on are not available, then people may reconfigure their pattern of relationships or may switch to using the Internet (the information and communication technological infrastructure) to interact with others.

Our view is that in times when the human infrastructure is disrupted, it must be rebuilt, reconnected, or "rewired". In many cases of environmental disruption, the technological information and communication infrastructure remained intact but it was the human infrastructure that was disrupted. The events of 9/11 and the 2006 Israeli-Lebanon war are examples showing that while Internet connections and cell phone reception were still available (after 9/11, the technological information and communication infrastructure in the World Trade Center area was destroyed while the surrounding area technological infrastructure was intact), the human infrastructure was severely affected. After 9/11, thousands were killed, entire companies such as Cantor Fitzgerald were destroyed, and many remained missing for days after the attacks (National Commission on Terrorist Attacks upon the United States, 2004).

The study reported in this paper is part of a larger research program that investigates how people can be resilient in war zones (Mark and Semaan, 2008). In this study we focus on how people can use the information and communication technological infrastructure to help build new human infrastructure. We investigated how people can use IT to support their daily activities amidst highly disruptive environments.

RESEARCH SETTING AND METHODOLOGY

Our research settings were two countries where residents experienced extreme disruption due to living in war zones. Our research participants lived in Israel during the 2006 Israeli-Lebanon war, and in Iraq, during the ongoing 2003 Gulf war.

It is a challenge to collect data in a war zone. Due to the limitations on travel in the war zone we chose to adopt a telephone interview method. Speaking with a foreigner face-to-face would put our informants at risk in a time of war, especially in Iraq. We therefore decided that telephone interviews would enable us to get access to residents in the area without putting the researcher or informant at risk. Interviews provide an essential opportunity to hear participants' perspectives (Spradley, 1979). We conducted a total of 85 semi-structured telephone interviews, ranging in length from one to four hours. 40 telephone interviews were done from Oct. 2006-July 2007 with Israeli residents living in Israel during the conflict in August 2006. All of these interviews were conducted in English. 45 telephone interviews were done with Iraqi residents who have lived in Iraq since

the beginning of the 2nd Gulf War in March 2003. These were conducted in both English and Arabic. Arabic interviews were translated by one of the researchers. All interviews were audio recorded and transcribed. When telephone communication was unavailable we switched to Skype, e-mail, or Yahoo Messenger in order to continue. In a sense we were experiencing the disruption from a distance, as when a technology was not working for our informants we had to switch to a communication technology that worked, or continue our interviews when the technologies were working again. The data was coded by the research team. We derived categories in our data related to the use of different types of infrastructure.

As our goal was to understand the interplay between the technological and human infrastructures in war zones, and given the limitations of access to larger populations for random sampling, we used a snowball sampling approach. We asked interviewees to recommend to us another person they knew who lived in the war zone and used IT. Finding Internet users was especially difficult in Iraq where only about 1% of the population are Internet users[1]. Our intent was to understand how technology adopters are able to utilize IT to rebuild relationships with those people on whom they rely. Our snowball sampling approach may limit the applicability of our results to the wider population. We sought to overcome this limitation by widening our sample as much as possible to include informants with a diversity of age, economic, and educational backgrounds.

The environment in the war zone

The environment in the war zones in both Israel and Iraq can be characterized as stressful, dangerous, and extremely risky in which to travel. We found that Israelis' daily lives were disrupted by warning sirens where they often had to go in and out of bomb shelters 8 to 10 times a day. The unpredictability of when an attack would occur, which area would be targeted, and how long it would last, meant that people were at risk both at home and while traveling during an attack. Iraqis described a range of disruptions to their daily activities. For example, their militia attacks on power stations and other government operated sources of energy led to a discontinuous source of electricity. Explosions and military operations in urban neighborhoods were experienced daily. These led to curfews and road blocks. Thus, household chores became sporadic and typically could not be carried out when there was no electricity or running water. Iraqis also found that they could not meet with family members or friends because of the restrictions on travel imposed by the curfews, roadblocks, and daily militia attacks. Their work life was also disrupted by lack of electricity and difficulties in traveling to work. Professionals especially were often targeted by militias and subjected to kidnapping and murder. This led many professionals to leave the country causing further disruption to the Iraqi human infrastructure.

RESULTS

We present cases based on our interviews that illustrate how people utilized the technological information and communication infrastructure in new ways when their human and physical infrastructures were impaired. For the most part, the technological information and communication infrastructure of Israel remained intact during the war. In Iraq the situation was quite different. Before the war the sanctions imposed on the country limited foreign trade with Iraqis and thus information and communication technologies were difficult to obtain. People had access to landline telephones and the radio, but the majority of Iraqis did not have access to foreign television stations via satellite. The Internet became available mostly to people working for the government prior to the start of the war. However, the connection was monitored and restricted to basic e-mail use and authorized websites. Following the war, due to the change in government and lifting of sanctions, an unrestricted Internet connection and satellites became available and cellular phones are now widespread. All but one of our Israeli informants reported an increased use of technology during the war. All of our Iraqi informants reported an increase in information and communication technology use during the war. Iraqis generally reported that they learned of the technology and how to utilize it through a combination of both trial and error and word of mouth.

Changing the use of infrastructure for safety

We discovered that people developed new ways of using available information and communication technology to improvise new coordination patterns and increase their sense of safety in their disrupted environment.

One example of how information and communication technologies were used in new ways is through the use of SMS for siren warnings. Some villages in Israel switched from audio siren warnings to using SMS to relay warnings. One person described that her village did not even have a working siren warning and they only received siren warnings through SMS on their cell phones. Sending SMS siren warnings enabled people to act

[1] (http://www.internetworldstats.com/me/iq.htm)

with more alternatives than they could with audio warnings. First, a cell phone notification informed them to take shelter. But importantly, these SMS warnings were also used as awareness notifications. When people traveled away from their homes they could still receive the SMS messages and could find out if their neighbors or if their homes were within siren range. People also passed these SMS siren messages on to others such as their children or parents to notify them of impending rockets. One informant described:

"The kibbutz that I'm living in was using SMS to tell people when to go into shelters, or whether it was possible to come out. And, there were a few complaints about the SMSs. Sometimes they weren't put out quickly enough for some people. And on the other hand, my daughter and my son who are living in Tel Aviv who have a phone from the kibbutz are also getting SMSs to go into shelters, because they were sent out to everybody."

Whereas the Virginia Tech shootings led many institutions to establish emergency message warnings (Gow et al., 2008) this is an example of how residents appropriated the SMS technology to spread the messages peer-to-peer. Thus, people utilized their human infrastructure in conjunction with the technological information and communication infrastructure to expand their capacity for time and location awareness of potential rockets. As people passed messages on with SMS to neighbors, colleagues, friends, and family, it enabled people to notify others about the environment independent of their physical location.

Another case is from Iraq. Prior to the war Iraqis could freely travel on roads. When the war started, travel on roads became dangerous not only due to bombings but also roadblocks. At the time of our interviews various sects and political parties constructed roadblocks and our informants reported that they could not distinguish whether the roadblock was set up by the government or the U.S. or operated by militia. Roadblocks presented challenges for residents. Not stopping at a roadblock was dangerous but at the same time if the roadblock was set up by a political party or sect different than the traveler it could have severe consequences for the traveler (Loyn, 2007). In order to travel to work and to attend classes our informants described how they started to use cell phone networks in which individuals would call others within their community (e.g. their neighborhood, workgroup, or university) who they knew would be traveling the same route that they had, in order to help others avoid dangers and delays they had encountered. Students would call to inform other students that there were no classes because of roadblocks or explain less time consuming alternate routes. One student described that this network helps him decide which direction is the safest to travel. An engineering student explained how he utilizes his cell phone not only to reassure his family of his well-being but also to stay informed of cancelled classes, e.g.:

"…a friend of mine calls me, and says I'm in college now and nobody's here, so you don't have to come, for example. Or like he tells me if there's no school… sometimes they postpone it... those kinds of things."

This use of cell phones shows again how people drew on the technological information and communication infrastructure to pass on critical information to others in their human networks about safe routes.

Our informants also reported using cell phones for psychological reasons to feel safer while traveling. For example, one informant, who is European, was working in Israel when the conflict broke out, and chose to remain. His workplace was located in the north of Israel which received rocket fire. He had a choice to return to Europe but chose instead to continue his job in Israel because as he explained, he really enjoyed the work and his colleagues. He described how he used cell phone and a web cam to communicate with his family in Europe before and after work, and before going to bed. He explained:

"It was... my family, my relatives they call me in the morning and ask what I'm doing and if I'm going to work. They call me, because its 7:30 and they know I leave then. 45 minutes later they call me again to see if I got to work. And the same for the way back."

Other informants reported using their cell phones more heavily during the war to call relatives before they left. One informant called home to his wife to ask when the last rocket hit. Based on this report he then judged when to drive (even though rocket patterns follow a stochastic process). Another informant used what she described as a "*cell phone battle plan*" to call her friend to coordinate picking her up. Her goal was to minimize the time on the road where she could be a target for rockets. She described:

"I called my neighbor. We called when we were close. I'm 30 seconds from her house, so we didn't have to wait outside her house. During shopping we ran inside a bomb shelter. Running a mission through enemy lines. Never occurred me to do that. This became an organized cell phone battle plan."

These examples illustrate how informants utilized the technological information and communication infrastructure to connect to others in their human infrastructure to help them be psychologically resilient in the environment. In this way it enabled them to travel.

Restructuring social and work practices by changing reliance on infrastructure

Informants in both of our countries reported that they changed their mode of interactions with friends and family, from meeting far less face-to-face to using technology to interact. This change was most pronounced in Iraq where people were accustomed to meeting face-to-face. Informants described how before the war they could go out at night to socialize. Social clubs were very popular. After the war started, potential bombs or insurgents posed a high threat to security during travel. In addition, the level of trust in meeting new people declined rapidly as strangers could be insurgents, spies, or terrorists. Even students at the university reported that they did not trust other students. As a result people began to use email, Instant Messaging, social networking sites, and Internet chat rooms to socialize. Medical students reported starting an online forum to discuss coursework, which was valuable especially if students were not able to physically attend class.

The Israelis also reported changing their social practices from meeting face-to-face to online and telephone interaction. All our informants reported using cell phones to a far higher degree during the war than before or after the war. When people went into shelters they made a series of short phone calls to close friends and relatives to let them know they were safe. However, they also restructured their social practices as well. Forty percent of our Israeli informants started completely new practices of blogging, sending long emails to distribution lists, and posting to Internet forums.

When people could not physically travel to work they also developed new virtual work practices. Working with colleagues online instead of meeting face-to-face enabled people to continue to work independent of their disrupted physical environment. Though virtual work practice is common in many western cultures, especially in globally distributed organizations, virtual work practice was very new for our informants. For example, five Israeli researchers were able to continue working on a research article with laptops and Internet connections, even though they were all constantly changing residences. An Israeli army reservist was able to seamlessly continue to work with his colleagues when he was called into the army. A CEO of a small company was able to continue working virtually as she continually changed residences. Informants in Israel reported that they were able to continue working even in bomb shelters with laptops and Internet connections. Some described how their international colleagues did not know that they were interacting from a bomb shelter. In fact, as some informants described, it was precisely their aim to create an impression that they were resilient in work and not affected by the physical disruption in their environment.

Iraqi informants also reported switching to virtual work practices to be resilient. An informant who is a journalist reported that two reporting groups in northern and southern Iraq began to use the Internet and cell phones to communicate rather than traveling across the country. Other journalists informed us that Internet access at home allowed them to extend their working hours beyond the limit imposed by the curfew and daylight hours by continuing their work from home. Other professionals reported that they could continue working using their laptops even when there was a power cut.

Thus, the human infrastructure as it existed prewar was not available due to the difficulty in travel and for Iraqis, also due to the degradation of trust. We found a general pattern in our data that our informants utilized the technological information and technological infrastructure in new ways to continue their former prewar practices of socializing and working. Online interaction led to a restructuring of the human infrastructure for some informants as they even met new people online. Informants were thus able to rebuild their human infrastructure by relying more on the technological information and communication infrastructure.

IMPLICATIONS

Work organizations have given attention to developing effective plans for coping with major environmental disruptions, e.g. short term plans for evacuation and saving lives, protecting buildings from further harm, and longer term plans for rebuilding the technological information and communication infrastructure. What is less common, however, are for organizations to consider plans that exist for rebuilding the human infrastructure. Our data show that repairing the human infrastructure through using alternative resources is an important consideration for maintaining the well-being of people who are facing continual threats in their society. This includes enabling people to negotiate safe travel as well as in continuing familiar routines and practices of socializing and working.

Virtual work and social practices enable a society to be robust against many types of physical disruptions. In our study we discovered that if the technological information and communication infrastructure is intact then it provided a range of alternative resources for people to continue to act. If the human or physical infrastructure is impaired then it would be effective to achieve robustness by enabling functions to be done over the Internet, as work and social practices can continue irrespective of location.

Although the Internet and mobile technologies are becoming a global phenomenon, in many countries, such as

Iraq, the Internet is used by only a small percentage of the population. One of the challenges new technology users face is the steep learning curve involved with understanding and being able to utilize such technologies. This may explain why many found new technologies available to them, such as the Internet, difficult to adopt. In order to ease this transition and spur adoption prior to and during a disaster, we offer some recommendations. Interfaces can incorporate local cultural expressions to aid learning. New methods of support can be developed to give users more details regarding their expectations. Our Iraqi informants reported learning to use technologies from friends and family who were already familiar with them and social networks could be utilized to support adoption. Virtual support from others in their network, as well as tutorials adapted to a culture, could prove useful to help train people in technology use.

The use of mobile technologies continues to grow globally and their use during disruptions becomes increasingly important. When the physical environment is impaired, people become more reliant on mobile devices to determine the safety of friends and family, to help others navigate through dangerous terrain, and to ask others for information about safe routes (Mark and Semaan, 2008). Today, these technologies are becoming more advanced as many are now equipped with Internet capabilities and GPS. In the United States, for example, people can use their GPS-enabled cellular phones in order to map driving routes, and these devices will automatically provide alternate routes when heavy traffic exists. Similar technologies should be used in disrupted environments. A cell phone with GPS could warn people where roads are not passable. The way in which these technologies populate data should take place either automatically through electronic means or manually, depending on the disruption and whether or not such information should not be released to the public, so as to prevent malicious behavior. Also, when a countrywide mandate goes into effect, such as a curfew or a bomb alert, people should be notified via their mobile devices.

When disasters strike, oftentimes various aspects of the technological information and communication infrastructure may fail. Whereas in Israel the technological information and communication infrastructure remained intact throughout the duration of the conflict, this was not the case in Iraq. Our informants reported that the wireless Internet connection was unstable, and that their mobile devices did not always have service. More reliable and affordable means of communication must become a high priority for civilians experiencing disruption.

CONCLUSIONS

Studies of disasters have generally focused on coordination through centralized channels. Our study contributes to bringing attention to the role of residents in appropriating IT to act in environments that have threats. We are aware of the limitations of snowball sampling in our study and for future studies would recommend the use of a random sampling of the population for interviews, if the physical conditions allow this.

Overall we found that people strove to repair human infrastructure despite their awareness of the dangers of their physical environment. This case highlights the need people have to repair their human infrastructure and further emphasizes the importance of developing and maintaining a technological information and communication infrastructure that will help residents do so.

ACKNOWLEDGMENTS

This research was supported by the National Science Foundation under grant no. 0712876. We thank our informants for their time. We also thank our anonymous reviewers for their comments.

REFERENCES

1. Gow, G.A., Townsend, D., McGee, T., and Anderson, P. (2008). Communication technology and campus safety: Critical sociotechnical concerns for emergency messaging at Canadian universities. *Technology and Society*, 2008. ISTAS 2008, 1-5.
2. Kendra, J. and Wachtendorf, T. Elements of resilience after the World Trade Center disaster: Reconstituting New York City's Emergency Operations Centre. *Disasters*, 27, 1, (2003), 37-53.
3. Lee, C., Dourish, P. and Mark, G. (2006). The Human Infrastructure of Cyberinfrastructure. *Proceedings of the ACM Conference on CSCW (CSCW'06)*, Calgary, Canada, 483-492.
4. Loyn, D., Local heroes: risk-taking in Iraq. *British Journalism Review*, 18, 2 (2007), 21-25.
5. Mark, G. and Semaan, B. (2008). Resilience in Collaboration: Technology as a Resource for New Patterns of Action. *Proceedings of the ACM Conference on CSCW (CSCW'08)*. ACM Press, 137-146.
6. Merriam-Webster Online Dictionary, (2008). Retrieved December 29, 2008, from http://www.merriam-webster.com/dictionary/infrastructure.

7. National Commission on Terrorist Attacks upon the United States, Heroism and Honor, U.S. Congress. August 21, 2004.
8. Palen, L. and Liu, S. (2007) Resident communications in disaster: Anticipating a future of ICT-supported public participation, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 727-736.
9. Shklovski, I., Palen, L. and Sutton, J. (2008). Finding community through information and communication technology during disaster events. *Proceedings of CSCW'08*, November 8–12, 2008, San Diego, 127-136.
10. Spradley, James P. (1979). *The Ethnographic Interview*. San Francisco: Holt, Rinehart and Winston, Inc.
11. Star, S.L. and Ruhleder, K. (1996). Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research*, 7(1), 111-134.
12. Vieweg, S., Palen, L., Liu, S., Hughes, A. & Sutton, J. Collective intelligence in disaster: Examination of the phenomenon in the aftermath of the 2007 Virginia Tech Shootings. *Proceedings of the 5th International ISCRAM Conference*. Washington, DC, USA, May 2008, 44-54.