Crisis Rooms Are Ambient Intelligence Digital Territories

Irene Mavrommati[1] and Achilles Kameas[1,2]

[1] Computer Technology Institute, Kazantzaki str, University Campus, 26500 Patras, Hellas
[2] Hellenic Open University, 23 Sahtouri str, 26222 Patras, Hellas
{mavrommati, kameas}@cti.gr

Abstract. The study of Digital Territories provides a way to conceptualize the interactions happening in Pervasive Computing Environments. This paper will address Crisis Rooms as Digital Territories. Based on the concepts stemming from Digital Territories we will attempt to give a high level overview of issues that can be applicable in the context of the future Crisis rooms and of the interactions that happen within them.

Keywords: Crisis Rooms, Digital Territories, Human Computer Interaction, Ambient Intelligence Environments.

1 Introduction

Crisis management involves identifying a crisis, planning a response to the crisis and confronting and resolving the crisis. Crisis management can be applied in almost any field of endeavor, but it is most commonly used in international relations, political science and management. Due to the large number of considerations involved in many decisions, computer-based Intelligent Decision Support Systems (that try to realize some human/cognitive decision making functions) have been developed to assist decision makers in considering the implications of various courses of thinking.

According to ISTAG [5], Ambient Intelligence is a vision that places human beings at the centre of future development of the knowledge-based society and ICTs. AmI space consists of a set of technologies, infrastructures, applications and services operating seamlessly across physical environments (e.g. neighbourhood, home, car); thus spanning all the different spheres of everyday life. Physical space becomes augmented with digital content, thus transcending the limits of nature and of direct human perception. A new term is needed for this new kind of space, which captures its dual nature. The term "digital territory" (DT) has been coined in an attempt to port a real world metaphor into the forthcoming synthetic world.

The Ubiquitous presence of information is becoming increasingly prominent; Crisis Rooms evolve into digital environments that have a hybrid nature (digital and physical).

Visualization technologies, multimodal interfaces, collaborative tools for remote, distributed decision-making are key to a rich landscape of information. Physical space that is augmented with digital capabilities, is providing appropriate information for situated decision making. Crisis rooms are Digital Territories that act as the physical

C. Stephanidis (Ed.): Universal Access in HCI, Part II, HCII 2007, LNCS 4555, pp. 151–157, 2007.

point of convergence where decision makers converge to learn, consider and decide. A *Digital Territory* is an ephemeral AmI space [3]: it is created for a specific purpose and integrates the will of the owner (an individual or group operator) with the means to achieve it (including infrastructure, properties, services and objects) within an AmI space. A Digital Territory can be composed of sub-spaces, which are determined with respect to their services, usage, etc. A territory is usually a continuum in space; the real and digital elements of Digital Territory however, may co-exist in disparate locations (in the end, any digital element is recorded on a hard-disk or other medium which has a specific physical substance and location – although the latter may change with time, i.e. if the device is mobile). The substitute for continuity in Digital Territory is proximity; in the case of crisis management, proximity is defined as being analogous to the degree of relationship to the crisis. The elements of a Digital Territory are active, as opposed to the usually passive objects found in real world territories. Transient elements, like activities or procedures, can now become elements of Digital Territory.

2 Crisis Management Requirements

The 'total design' of Crisis management rooms (i.e. the design of physical and digital space and interactions) determines how the involved actors act (as individuals or groups), navigate and react to information [4]. It includes all aspects of Digital Territories, such as ownership, visibility of information, communication with the environment, etc. For example, the design of borders and markers (digital and physical) of a Crisis room affects how secure the exchange of information is.

Crisis management is primarily concerned with the following issues:

- Preparation and management all operations from response to recovery
- Event and incident tracking
- Personnel, material and resource management
- Emergency operation plans and procedures
- Manage personnel resources
- Document and track Incidents and Commands

Efficient and effective features for crisis management are considered the following:

- Tracking events
- Log task status to completion
- Deploy resources, then monitor, track and demobilize them
- Create standard operating procedures, checklists and notification lists
- Track resources and inventory, including strike team members
- Geographical mapping interfaces allows for geo-spatial representation of data

Usability of the crisis room environment and crisis management software is therefore very important. Robustness of the software and equipment, and design so that both of them leave no room for error, is crucial. The controls and information

visualization embedded in the environment –the crisis room- has to be quick to learn and master, to use and navigate in. The same applies for the software used of course, and the way it locates and interacts with the physical environment of the room.

The security of the crisis management information is of utmost importance, while at the same time the system should allow certain information disclosure to trusted parties and actors resolving the crisis.

Crisis management is facilitated by an array of crisis management software. Rooms that are specially designed, engineered and equipped, the so called crisis rooms, bring the decision actors and teams together and facilitate them in terms of information, communication, action planning and deployment, tracking completion and receiving feedback from each action, in order to resolve the crisis.

3 The Crisis Bubble

Modern Crisis Rooms are physical spaces augmented with information and communication technology infrastructure. In the case of crisis management, one could define the crisis room as being a Digital Territory. A territory has a measurable quantity of elements which are contained within its borders. Borders are no more defined as "lines" to traverse or not. *Borders* are conceived as spaces "in-between", spaces of negotiation. *Markers* are a way of defining / denoting the boundaries, the borders and the points of negotiation and crossing.

In fact, one could apply the concept of Virtual Residence in the case of Crisis Rooms [2]. The basic elements of a Virtual Residence, that is, a "connected" room or space, the online lives of people and mobility and interoperability between different AmI environments, can be applied to Crisis Rooms as well. A Crisis Room occupies one or more physical rooms – in that way, we can model access to activities that take place in distant locations, where, for example, some member of the crisis management committee are located, or the premises of the organization under crisis. The people or organisations that own or are part of bubbles have their data online and use computers to implement several procedures. Finally, support for mobility between physical spaces or information servers and interoperability between activities (modeled as bubbles) is a prerequisite for any crisis management process.

A (digital) *bubble* is a temporarily defined AmI space within a Digital Territory that can be used to limit the information coming in or leaving with respect to a specific activity. As a direct consequence to its relationship with Digital Territory, the bubble concept clusters together all the interfaces, formats, rights and agreements etc. needed for the management of personal, group and public data and informational interactions that relate to this activity. Such contextual activity can be based on privacy, personalization, priority, location, membership, ambience, social circumstances, and time.. *Ownership* depends entirely on the purpose the bubble serves. The owner claims bubble territoriality in order to regulate the Digital Territory environment. The owner of a Digital Territory bubble can be a single person, a group, or an agent.

Within this Digital Territory, several bubbles co-exist more or less closely related to the crisis. The most important among them is the crisis bubble, which contains all data and procedures related to the particular crisis. This bubble is transient; it lasts as

long as the crisis lasts and then is dissolved. Other participating bubbles are those of the actors (people, organizations, agents etc) involved in the crisis. These contain the personal or other data of their respective owner and usually will persist even after the crisis is over.

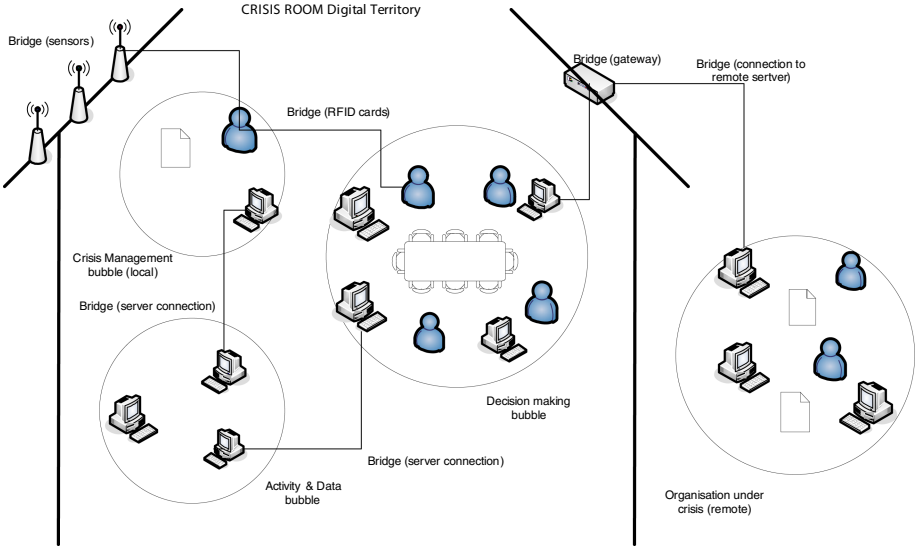

Fig. 1. Interactions within Digital Territories

Specific Interactions in Digital Territories that thus apply to Crisis rooms are (figure 1):

- interaction between bubbles and environment (through bridges)
- interaction between bubbles and markers
- evolution of bubbles as a result of these interactions
- interaction as part of the negotiation process for the specification of markers and borders
- interaction related to identity, privacy and trust negotiation

Each of the actors can be perceived as defining a 'bubble' space that contains the personal or other data of their respective owner and will usually remain even after the crisis is over. Crisis actors can isolate by closing the digital links, i.e. by manipulating the transparency of their individual bubble, so that they are made non accessible and not visible. Decisions, taken as a result of negotiation between the bubble entities, can have a direct digital and communication effect. Tracking and registration of events (physical as well as digital) is facilitated, as every action –upon the elements of the physical tangible environment- has a digital counterpart within the context of a Digital Territory.

4 Crisis Room Bridges

Bridges between physical and digital are actually elements/components of AmI spaces linking the physical and the digital and facilitating exchange of information in Crisis Room bubbles or between the Crisis Room and other environments. They may be combinations of physical and digital media, often so interwoven with everyday life that they are no longer noticed as special, novel or distinct. Bridges are discrete elements disposing of certain autonomy in their conception and internal structure. Sensors, actuators and RFIDs are examples of bridges between the physical and the digital. When one builds a bridge between the physical and the digital space, it is in fact a bridge between activities that take place in remote physical spaces in the same time. Examples of current technology and artifacts that can be used as bridges are: location based services, RFIDs, bio-implants, biometrics, user interfaces, and CCTV's, etc. When one builds a bridge between the physical and the digital space, it is in fact a bridge between activities that take place in remote physical spaces in the same time.

Bridges are of interest when they enhance Digital Territories -and therefore Crisis Rooms as such- by supporting modification of contained relationships, newly-emerging requests of DT members and enable the creation of (new) complex DTs. The need to create bridges arises from the generation of new, additional or transformed data, the need to transfer information, as well as the need to pass to a different level of hierarchy, either within a DT or between different DTs in AmI spaces. When created for generating complex DTs (i.e. by DT inter-connection), they allow consideration of new links that where not possible before.

Bridges within the context of Crisis rooms can be considered as the linking elements between the sub-elements of a crisis situation. These can be in a digital form or a physical form –for example an RFID tagged card. Via them a tangible interface to the crisis software can be facilitated for example, for reasons of speed, efficiency, geographical mapping of data visualization, etc. Resources can be inventorised and tracked easier by using augmented interfaces to the digital data representations.

5 Human Computer Interaction Issues in DT Crisis Rooms

New elements that are introduced by the nature of living and interacting within an Ambient intelligent environment lead to new HCI paradigms. Some of the issues that have an impact in AmI HCI research practice [**Error! Reference source not found.**] -and therefore the augmented space of Crisis Rooms- are:

1. A shift in the nature of interaction

Interaction in Ambient Intelligence Spaces can range from explicit to implicit interaction. Unintended user actions on the environment may result in unintended control and manipulation of the ambient applications. Ambient Intelligence Environment vision implies less direct and less conscious user input than in the current systems. This in turn raises issues of the appropriate level of transparency and visibility to the workings of the system. In concepts borrowed from Digital territories

that would imply a focus to the realization of a moderated transparency level in the visualization of the Bubble metaphors, as well as possibility for the information visualization of the available and the active bridges.

2. Different interaction channels (shift in the nature of input and output devices)

The context of DT in Crisis Rooms implies the introduction of tangible manipulation controls within the environment that interface with the information and its manipulation, alongside to the Crisis management software. A value to this approach could be the replacement of complex command languages with actions from manipulating directly the objects, and making use of multimodal interface combinations to interact with the system. Crisis room and the crisis management software can be perceived in this context as one DT entity, where the elements of the physical and the digital are interacting.

3. The role of intelligence

Actors coming into play within the crisis management are agents (that can be human, software, or their combination), who are collecting and comparing data, benchmark against similar past situations and can present informed decision choices. These can also be intelligent software agents within the Digital Territory environment, facilitating actions and communication, and specific applications. In such case unexpected behavior –resulting agent intervention- that may surprise the user *must* be avoided; visibility on the workings of the intelligent system and its rationale, should be available upon request, as well as an overwrite function for the agent (the overall off switch).

4. Visibility, Reversibility of action, Error tolerance

Feedback should be provided for actions upon the physical environment which affect/manipulate digital aspects of the crisis. Syntactic correctness of sequences of actions has to be checked at all times, in order to appropriately inform users, so as to avoid errors before they are made. To be able to undo actions (reversibility of actions) is also very important in the case of error, and in order to avoid extensive delays in the handling of the crisis.

6 Conclusions

Crisis rooms involve a merge of the physical and the digital world, which come together in the context of a crisis management situation. Therefore Crisis rooms of the future will increasingly resemble Ambient Intelligence Spaces –targeted to handling specific situations. The Digital Territories study has developed concepts for this merge of the physical and digital worlds. The concepts of Digital Territories can be useful to the conceptualization and design of future Crisis rooms. In particular concepts such as borders and markers and metaphors such as bridges and bubbles can provide useful insight into the design of future crisis rooms.

References

1. Altman, I.: The environment and social behaviour: privacy, personal space, territory, crowding. Brooks/Cole Publishing Company (1975)
2. Beslay, L., Punie, Y.: The virtual residence: Identity, privacy and security. The IPTS Report, Special Issue on Identity and Privacy, No. 67, September 2002, pp. 17–23 (2004)
3. Daskala, B., Maghiros, I.: Digital Territories. Proceedings of the 2nd IET International Conference on Intelligent Environments (IE06), 5-6 July 2006, Athens, Greece. Published by IET, pp. 221 – 226, vol. 2 (2006)
4. Halkia, M.: Panel description UAHCI2006, Beijing, China (July 2007)
5. Advisory, I.S.T.: Group Working Group Report, Ambient Intelligence: from vision to reality [For participation – in society & business]. Available at (2003), ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf
6. Mavrommati, I., Darzentas, J.: An overview of AmI from a User Centered Design Perspective. Proceedings of the 2nd IET International Conference on Intelligent Environments (IE06), 5-6 July, Athens, Greece. Published by IET, pp.81–88 vol. 2 (2006)