J Syst Sci Syst Eng
DOI:
ISSN: 1004-3756 (Paper) 1861-9576 (Online)
CN11-2983/N

RESILIENCE 2.0: COMPUTER-AIDED DISASTER MANAGEMENT

Gerhard Chroust[1] **Georg Aumayr**[2]

[1]*Institute for Telecooperation, Johannes Kepler University Linz, Austria*
Gerhard.Chroust@jku.at (✉)
[2]*Johanniter Österreich Ausbildung und Forschung, Vienna, Austria*
georg.aumayr@johanniter.at

Abstract

Many factors (larger population, more dependency on technology, more human-caused interference in the natural systems and equilibria, climate changes, ⋯) contribute to the seemingly growing number and severity of disasters. Additional exaggeration is generated by public media. As a consequence Disaster Prevention and Disaster Management must be given increased attention. The ultimate goal of Disaster Management is resilience of the affected system and thus the adequate and acceptable survival of the affected population.

We discuss system behavior in the case of an assault or disturbance: from being fragile (loss of their functionality due to the assault) to being resilient (having the capacity ⋯ of bouncing back to dynamic stability after a disturbance), or even antifragile (being able to "learn" so as to improve disaster resilience).

Resilience 2.0 identifies a new paradigm: modern Information and Communication Technologies (ICT) are employed as a basis for enabling and improving resilience of a system. ICT provide the basis for sufficient preparation before an assault, for quick recognition of, and for effective, efficient reactions to disasters. Only the coordinated intra- and interphase deployment of ICT promises sufficient success and can bring resilience to currently as yet fragile systems. We discuss stressors (time and performance pressure, physical and psychological stress on personnel) and problems due to damaged ICT-platforms and communication infrastructure. The basic message is that computer-aided Disaster Management is able to offers a new level of reactivity: *Resilience 2.0.*

Keywords: Disaster, vulnerability, resilience, human reaction, hazard, threat, systemic reaction

1. Motivation

Observing public news media a feeling of foreboding arises that more and more disasters of different kinds endanger the foundations of our society. These seem to occur with more frequency and create more catastrophic situations (Aumayr et. al. 2015, Chroust & Aumayr 2015). They are related to the increased number of global inhabitants and to the modern way of life, to human impact on the environment and last not

© Systems Engineering Society of China and Springer-Verlag Berlin Heidelberg 2017

least to a higher quest for security and safety.

We want our systems to be resilient, generally speaking (see section 3.2 for details) that the systems have "*the capacity… to bounce back to dynamic stability after a disturbance*" (Francois 2004). In order to ensure both resilience and the well-being of societies (small or large) we have to study the various shapes and appearances of disasters and – given our high standards of technology – employ modern technology in the service of Disaster Management.

Above calls for answers to several questions:

• What is a disaster? This calls for definition and for classification.

• What are the phases of a disaster and corresponding response activities? This calls for planning and information transfer.

• What are the typical types of reaction of a system in case of a disturbance? This calls for scientific analysis and research.

• What are the temporal parameters of a disaster both with respect to a disaster's inception and the corresponding human responses? This demands observance of both nature and human beings.

• In what respect can modern Information and Communication Technologies (ICT) help in order to improve Disaster Management? This calls for understanding of technology and creative application of it.

The paper is structured as follows: Chapter 2 discusses the disturbances, their types and behavior, Chapter 3 analyses reactions of humans and systems, while Chapter 4 explains the principles of Disaster Management which leads to Chapter 5 investigating the use of ICT in Disaster Management.

2. What Is A Disaster?

2.1 The Origins of Disasters

Disasters are the result of unfavorable combination of three major factors (Fig. 1) as explained by following Khan et al. (2008):

Hazard: This is "a dangerous condition or event, that threaten or have the potential for causing injury to life or damage property or the environment".

Vulnerability: This is the property of "a community, structure, service or geographic area [that] is likely to be damaged or disrupted by the impact of a particular hazard, on account of their nature, construction and proximity to hazardous terrains or a disaster prone area."

Capacity: This describes the "resources, means and strengths which exist in household and communities which enable them to cope with, withstand, prepare for, prevent, mitigate or quickly recover from a disaster".

Figure 1 Factors contributing to a disaster

Depending on the individual's view of life and world view as a whole there are different ways of considering and defining a "disaster" (Tierney et al. 2001, Quarantelli 1985):

the functionalistic or effect-based perspective: "A disaster is a natural or man-made hazard that has come to fruition, resulting in an event of substantial extent causing significant physical damage or destruction, loss of life, or drastic change to the natural environment. A ⋯ tragic event with great loss stemming from events such as earthquakes, floods, catastrophic accidents, fires, or explosions" (Wikipedia 2013, keyword 'Disaster'). Nowadays one also includes large financial losses.

loss of system viability M. Mrotzek (Mrotzek & Ossimitz 2008a, Mrotzek 2009) identifies a disaster as any event in which the system transgresses the boundaries of what is considered to be acceptable or safe (see fig. 3).

the social disruption: (Tierney et al. 2001) and (Quarantelli 1985) consider the vulnerability of the built environment and the social disruption of the affected populations; referring to Bolin & Standford (1998): "*Vulnerability concerns the complex of social, economic, and political conservations in which peoples' every day lives are imbedded* ⋯". A break-down and destruction of a civilization (Diamond 2005) would be the ultimate result.

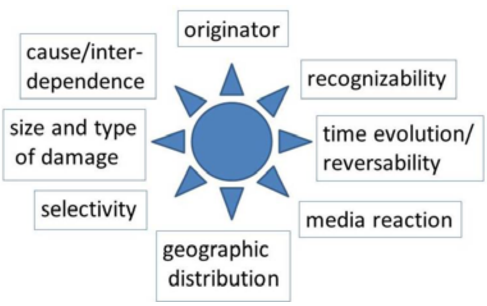

Figure 2 Factors contributing to a disaster

the social/political construction: Quarantelli (1985) and Kreps et al. (1989) cited by Tierney et al. (2001) identify disasters as social or political constructions: disaster events and their impacts do not exist sui generis but are products of social definition. They are a social construction, i.e. "*disasters are in the eye of the beholder*".

The first three cases imply that the affected society needs external help.

2.2 Classifying Disasters

Disaster can be classified according to many different dimensions, the most prominent ones are shown in fig. 2 (Chroust et al. 2011):

Originator: Traditionally a broad distinction is made between man-made, man-triggered, and natural disasters. Man-made disasters are further divided into technological and mass violence disasters (Norris et al. 2002). Looking at past catastrophes it must be admitted, however, that this criterion has lost most of its distinctiveness. Natural disasters frequently involve a human element: For example, the volcanic eruption of Mount Eyjafjallajökull (In Iceland 2010) was a purely natural disaster but the effect of the volcanic ash was a complete break-down of air traffic with considerable consequences for the economy. Without air traffic it would not have been seen as a disaster. Similarly the earthquake in 2011 in Fukushima, Japan, was a natural disaster which triggered a disastrous tsunami. Due to the interruption which occurred in the electricity supply by the tsunami the atomic reactors came to a highly critical state and made a technological disaster.

Cause/interdependence: A classical distinction is based on the cause of disasters, for example the acronyms CBRN (chemical, biological, radioactive, nuclear (Chroust et al. 2009b)) or ABCDEF (atomic, biological, chemical, data-network, electromagnetic, release (from the German word "Freisetzung") of energy) etc. are used to classify the dangers and the precautions/reactions to be taken (Ossimitz & Lapp 2006)). Other causes can be volcanic, epidemiological, avalanche, earthquake, etc.

Size and type of damage: Various classifications for systems exist, identifying the 'size' of the disaster (small/large) and the resulting damage (monetary, infrastructure, and humans).

Geographic distribution: What is the extent of land/air area which is affected (local, regional, international, global)?

Time evolution/reversablity: How does the disaster start (e.g. slow or rapid onset) and how does it develop over time? With respect to warning potential victims the lead time before the catastrophe's onset (warning time!) is of essential importance, e.g. slow or rapid onset (Tierney et al. 2001) (Skrbek & Kviz 2010). This is strongly linked to the notion of recognizability (see below). Mrotzek (Mrotzek and Ossimitz 2008a, Mrotzek 2009) discusses different temporal behavior of catastrophes (Fig. 3), also various characteristics of a disaster's change over time (growing, e.g. atomic plants spiralling out of control), shrinking (floods receding), converting (snow being converted to water posing a different type of threat, $\cdots$). Reversability of the effects of the disaster is of special importance.

Recognizability: Not all disasters can immediately be recognized by our naked sensor apparatus. Typically atomic radiation is not felt immediately at all. Some of the disasters have only long-term detrimental effects (atomic radiation!). Thus humans do not have natural, semi-autonomous reflex patterns (e.g. as in the case of extreme heat). For these cases humans need to be equipped with special tools in order to recognize dangers, and have to be taught to use them properly (Chroust 2009a). Can one recognize it in hindsight?

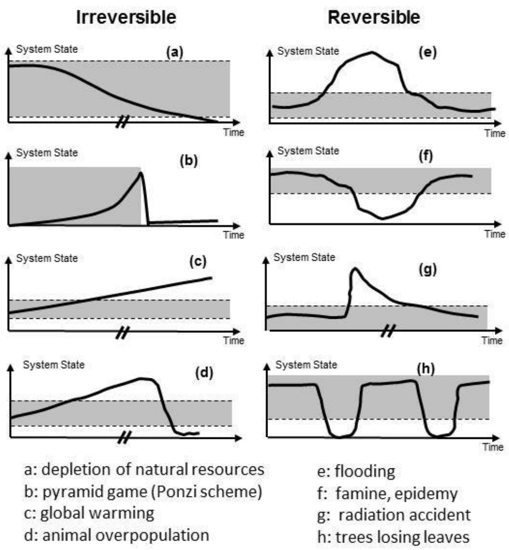

Figure 3 Factors contributing to a disaster

Selectivity: It is necessary to understand what and/or who is affected by the disasters. Some illnesses only afflict certain species (humans, some species of animals, $\cdots$). The neutron bomb does not destroy any buildings or artefacts and 'only' kills humans.

Media reaction: We also have to recognize the effect and the distortion of reports on disasters by the media. Does it make headlines, does it go into the news or is it largely ignored by the outside world? A speaker of the Austrian Red Cross regretted that in comparison to the Fukushima accident there are other disasters (even bigger ones especially with respect to human cost) which are practically ignored.

3. Reaction Types in Case of an Assault

We have to distinguish between two essential aspects, the reactions of the individuals and those of the system in its entirety (be it a small community or a large nation).

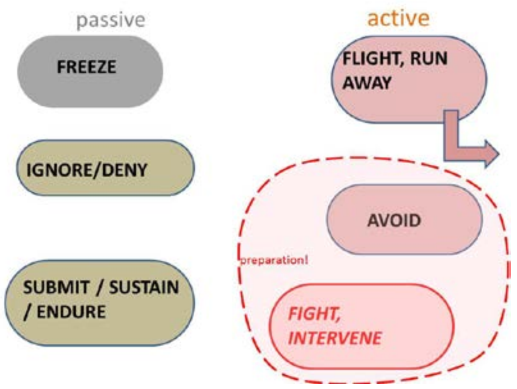

Figure 4 Fundamental (Re-)actions

3.1 The Individual

Humans and animals (individuals and organizations) show several basic types of reactions (Fig. 4) when confronted with a dangerous situation (Chroust 2011).

Flight, Run away: This is one of the two alternatives of the classical response to a problem (fight-flight), if it is possible to flee.

Fight, intervene: This reaction intends to actively reduce/mitigate/eliminate the impending or existing danger. It is based on performing compensation actions which try to return the system or environment back to an (at least temporarily) acceptable state. The system would be only un-acceptable for a (relatively?) short interval and will then be transformed into a (potentially different) acceptable system again, see Fig. 5 and Fig. 7.

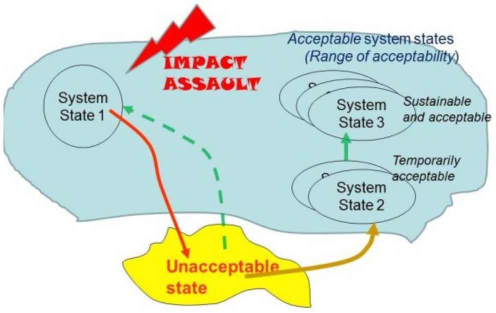

Figure 5 Acceptable/unacceptable system states

Freeze: In case of danger many animals completely immobilize their whole body showing no reaction whatsoever. For them this is a successful strategy with respect to certain predators: they would not eat dead animals or might not notice them due to the lack of movement. For humans this does not seem to be a viable strategy and is rather considered an inadequate reaction.

Submit/Sustain/Endure: In this case people do not try to fix, repair, change the system or situation but *to change/adjust themselves* in order to be able to live under the supposedly disastrous situation. 'Riding it out' as a strategy and sustaining a disaster (and not "running away") needs a certain frame of mind, and also includes a certain risk. Sometimes humans resort to re-interpreting the status of the system as 'non-disastrous' (Dörner 1996). The behavior is similar to Ignore/Deny, the difference lies probably in the motives. Motives which induce people to stay are (Tierney et al. 2001): the disbelief in the severity, fear of looting of their properties, waiting for other clan-members, ⋯ Obviously this approach is only sustainable if the system - despite its disastrous effects - has a certain kind of stability in its behavior and properties.

Ignore/Deny: Sometimes people simply ignore the immediate or upcoming danger, they act as though nothing has changed. This can be interpreted as an 'inner' flight. In the worst case this can be a sign of mental disorder. In Vienna we use a phrase to describe this state of mind: "*do not even ignore it!*" Dörner (1996) points out that in certain obviously disastrous situations the political leaders apply verbal camouflage to disturbing phenomena by coining special words like "minus growth" (=shrinking), "front line balancing" (= retreat of troops). An even stronger distortion of the truth is target inversion in which a negative outcome is interpreted as the goal ("this is the 'steal-bath' of the nation" (Nazi propaganda)), "many enemies - much honor".

3.2 Vulnerability Classes of Systems

Basically most stakeholders (probably excluding terrorists, anarchists, etc.) are interested in maintaining a system in a certain state of stability and security. This requires the system to possess a certain resistance against the consequences of disturbances. A disturbance causes the affected system to go into a different state, either temporarily or permanently. From there transitions to different states are possible (Fig. 6).

Holling (1986) adds: "*The size of the stability domain of residence, the strength of repulsive forces at the boundary, and the resistance of the domain to contractions are all distinct measures of resilience". [A system] has "the ability ⋯ to absorb changes of state variables, driving variables, and parameters, and still persist*".

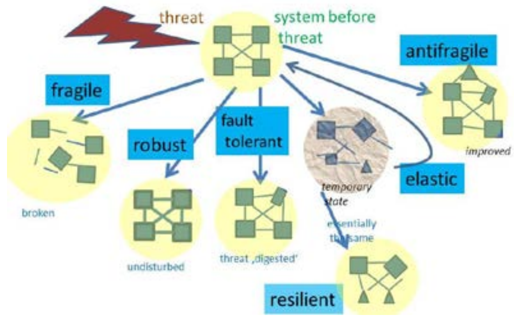

Figure 6 Vulnerability classes

With respect to the final state we can classify systems:

fragile: The system breaks/becomes non-existent for the future. In general fragility is to be avoided.

fault tolerant: The system has "the ability ⋯ to absorb changes of state variables, driving variables, and parameters, and still persist" (Holling 1986). For a limited set of pre-defined hazards ('faults') the system is able to cope with or handle the disturbance successfully. Fault tolerance is not sufficient in those cases in which full control or knowledge about the environment is not available/possible or certain hazards are not considered.

elastic: After a short time the system returns to its original state. Physics teaches us, that strictly speaking 100% elasticity is usually not achievable.

resilient: Resilience is *"the capacity of an adapting ⋯ system to bounce back to dynamic stability after a disturbance*" (Francois

2004).The system, when damaged, is able to be returned to an acceptable state, most likely not the same as before (Fig. 5). *Resilience* over a wide (and not even fully known) range of possible hazards is a highly desirable property of a system and therefore the most worthwhile objective of system design with respect to Disaster Management (Brose 2015). Resilience, however, like many desirable aspects of Disaster Management, cannot be had free of cost: it entails expenses and effort and needs preparation before a disaster strikes. Note that sometimes resilience is meant to be what we call elasticity (Wikipedia-english, keyword 'Resilience').

robust: The system is such that it remains unchanged by a disturbance, basically it is not affected. *Robustness* might be too difficult to achieve due to the cost and effort for the current system. Additionally maintenance and evolution of a system of this kind might become too difficult.

antifragile: Antifragility is "*the system's ability to create new conditions of fitness for itself whenever necessary*" (Francois 2004). The system is not only resilient but additionally "learns" to better counter a similar disturbance in the future, possibly becoming fault tolerant or even robust for certain disturbances (Taleb 2012). *Antifragility* often might be not achievable because its implementation might require too many additional complex system components or overhead in order to exhibit the learning effect.

Above classification is somewhat simplistic and idealistic, since a system may react in completely different ways to different types of hazards and threats. Additionally the duration of achieving an acceptable state can vary from hours to years. Finally the definitions strongly depend on the definition of the system boundary: A house itself might be rather fragile with respect to fire, but if we consider the city's fire brigade as a part of the threatened system, then it can be classified as fault tolerant or resilient, see Fig. 7.

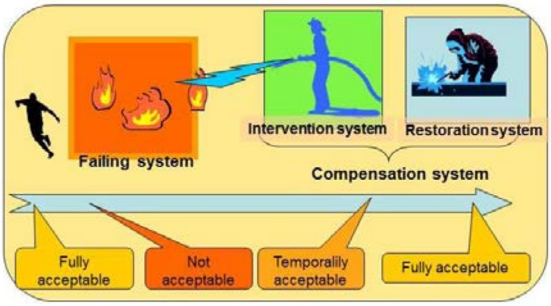

Figure 7 Intervention and Restoration System

3.3 Temporal Behavior of Disasters

Disasters can behave very differently over time. Fig. 3 show possible behaviors of disasters (Mrotzek & Ossimitz 2008b, Mrotzek 2009). The grey areas indicate the 'acceptable domain'. Behavior ranges from abruptly starting without any warning (e.g. comets, 'b' and 'g' in Fig. 3) to slow on-set disasters where it is even difficult to pinpoint the point-of-no-return turning a normal situation gradually into a disaster (e.g. global warming or floods, 'a', 'c' and 'd' in fig. 3). Even periodicity exists (trees losing their leaves in 'h' in fig. 3).

Some key timing parameters are:

- T_{ident} Time of identification of hazard
- T_{rec} Time of recognition of (expected) disaster
- T_{exp} Time of expected (EARLIEST) impact
- T_{lead} Time for preparation = $T_{exp} - T_{rec}$
- T_{alarm} Warning time = T_{exp} – NOW
- T_{set-up} Time needed to set-up intervention resources

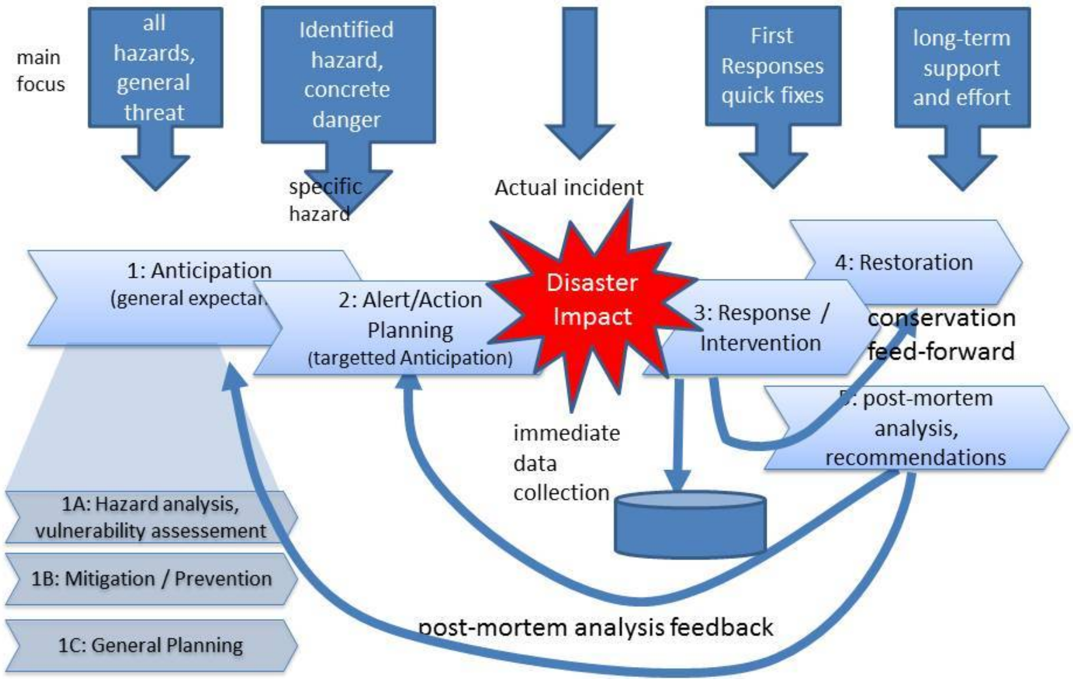

Figure 8 Disaster phases and corresponding response processes

4. Disaster Management

Several phases of Disaster Management can be identified, but the classifications, the demarcations between the phases, their names and the comprised activities are not uniformly defined yet (Tierney et al. 2001, Khan et al. 2008, McEntire 2007, INSARAG 2012). It can be hoped that the standard ISO 22320 (Lazarte 2013, ISO 2011) will bring some uniformity.

The Disaster Impact is the pivot point, although even there a definition might be difficult when we talk about slow-onset disasters like in Fig. 3 ('a', 'c' and 'd').

Fig. 8 shows the phases of Disaster Management together with the main information flows.

Phase 1. Anticipation: This encompasses all activities which are undertaken before any specific hazard becomes threatening (IFRC 2007b, a, McEntire 2007, Tierney et al. 2001). Three different tasks have to be considered:

1A: Hazard analysis, vulnerability assessment: Based on data concerning existing hazards the risks for a region/society must be analyzed by analyzing the vulnerabilities and the capabilities (IFRC 2007b).

1B: Mitigation/prevention: This encompasses any activities which can reduce either the chance of a hazard becoming dangerous or turning into disaster.

1C: General Planning Anticipatory measures and actions are taken: action plans, listing and providing necessary resources and equipment, organizing training, etc. for any anticipated hazards. This includes considering resilience and plans for the restoration phase.

Phase 2. Alert/Action Planning: In this phase a hazard has come to fruition. Plans or preparations are made as to how to react, to save lives or property, and decide how the rescue service operations can be coordinated and executed. This phase covers implementation and operation, refreshing of training, issuing of early warnings, building up response capacities etc. so the population will react appropriately when an early warning is actually issued.

Phase 3. Response/Intervention: This deals primarily with the rescue of people and restoring of the system to a temporarily stable state ('quick fixes') - in most cases with external help. This phase is the implementation of the action plans conceived in Phase 2.

Phase 4. Recovery/Restoration: The often long-lasting Restoration Phase aims at restoring the system to a long-term acceptable state (Chroust 2015) but also aims at reducing vulnerability and improving maintainability. It includes actions that assist a community to return to a sense of normality after a disaster.

Phase 5. Post-mortem Analysis and Recommendations: This is the path leading to future improvement by collecting, analyzing and aggregating lessons learnt, and making recommendations for the system in general and for the next Phase 1 in particular.

5. Resilience 2.0 and ICT Support

5.1 Utilizing ICT

Like most other human endeavors Disaster Management can profit from the application of Information and Communication Technologies (Svata 2012, Asimakopoulou & Bessis 2010), (McEntire 2007).

Resilience 2.0 identifies this new paradigm: modern Information and Communication Technologies (ICT) are used as a basis and even a precondition for resilience of a system and provide quick, effective, efficient, and sustainable Disaster Management for the different phases. All phases can be supported - sometimes even automated by use of ICT. Most of these technologies are also used in every-day business.

We see ICT essentially in two different roles (Fig. 9):

• ICT as the driver and mediator of *information* (Haddow & Haddow 2008), like Big Data analysis (Greengard 2014, Cruz 2005, Backfried et al.2013), Crowd Sourcing (Grifantini 2009), sensor technology (Filippoupolitis et al. 2008), simulation (Mrotzek 2009, Kelton et al. 2007, Pfahl 2005, SimRad.NBC 2009), virtual reality (Azuma 2004),

• ICT as supporter of *logistics*, i.e. the administrator of materials and equipment (Roth et al. 2012, McEntire 2007, INSARAG 2012).

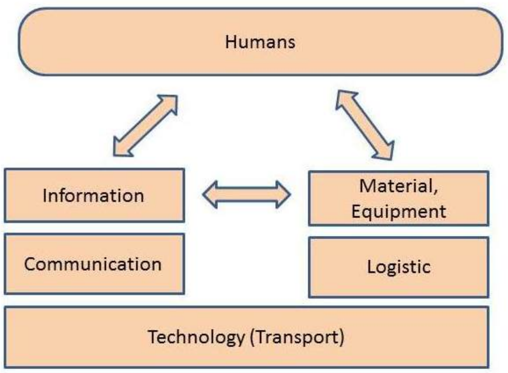

Figure 9 ICT Resources

An important aspect is that modern ICT allow the helpers 'to broaden the horizon' in several dimensions:

- *look into the past:* retrieve historical information on similar events,
- *look into the future:* simulate and predict the evolvement of disasters (e.g. like in Fig. 3),
- *look into the details:* identify small indicative changes (e.g. automatic measuring of small earth movements),
- *look to the side:* observe and take into account a much larger systems view of the environment.

5.2 Challenges for ICT during Response/Intervention (Phase 3)

Except for Phase 3 (see Fig. 8) the use of ICT for Disaster Management will not differ greatly from classical applications. Application and use of ICT in Phase 3 (Response/Intervention), however, encounters considerable additional problems. The difficulties result from the circumstances and the environment of responding to a disaster. In a nutshell these extraordinary difficulties stem often from the high priority of savings lives by preempting other important tasks, time and performance pressure, physical and psychological stress on personnel, damaged ICT infrastructure, unknown and/or adverse natural environment, etc.

Communication:

• communication equipment might be damaged, out of order, or reduced in its capacity

• Social Media interactions by mobile phones and internet connectivity might overload the available channels blocking disaster-relevant messages

• communication between helpers from different countries and cultures will add problems of understanding and cooperation

• agitation and stress might degrade the quality of observations and messages

Performance Stress:

• time pressure/preemption of tasks and procedures due to the urgency and priority of saving human lives

• missing, damaged, inadequate equipment

• incomplete and often misleading information for planning purposes

• incompetent, non-existing local support

ICT infrastructure:

• special precautions have to be taken to overcome damages to the ICT-infrastructures itselves: destroyed/damaged computer equipment, land lines and WLAN connections

• electrical power supply might be severely damaged or not-existent (black-out)

• overloading of WLAN capacity due to high-volume usage (social media!)

Personnel:

• psychological stress for all stakeholders (Bundesamt f. Bevölkerungsschutz und Katastrophenhilfe 2011)

• regular personnel might be incapacitated themselves or busy helping their own family and therefore not be available

• volunteers will probably be not sufficiently trained for operating complex ICT-equipment

• outside helpers will come from different regions, language groups, ethnicity and cultures creating problems in communication and cooperation

New methods and strategies:

• New developments in communication technology and the resulting effects on Disaster Management have to be taken into account for designing new strategies

• The broadening of communication loops between disaster relief staff (Manahl & Drechsler 2015) and disaster relief organizations improves efficiency

• Information exchange (Sackl et al. 2015) in new areas, e.g. Internet of Things (PublicSafety.NET 2015) or telemedicine (Aumayr 2015) have to be considered and employed in a systematic approach.

6. Summary

Resilience of systems is a highly desirable goal. In this paper we have shown the systemic aspects of disasters and have discussed the use of ICT in order to create/improve resilience of many of the systems our society depends on. Only the coordinated use of ICT in all 5 Phases promises sufficient success and the chance to turn many of our now still fragile systems into resilient systems. This aim requires investment with respect to funds and creative thinking and is a long range project.

We have also discussed that ICT itself is vulnerable to the imponderabilities of a disaster impact. This requires resilience considerations for the ICT infrastructure itself.

We hope that this paper will trigger an interdisciplinary discussion, perhaps also exhibiting new approaches and new methods and will improve the situation for humans affected in the case of a disaster.

Resilience 2.0 is here to stay and to be improved!

7. Acknowledgements

The foundations of this work was funded by projects supported by security program "Sicherheitsforschungs - Förderprogramm KIRAS" of the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT).

The authors also want to thank the reviewers for their help and support in improving the quality of the paper.

References

[1] Asimakopoulou, E. & Bessis, N. (2010). Advanced ICTs for disaster management and threat detection: collaborative and distributed frameworks. Information Sciences References, 2010.

[2] Aumayr, G. (2015). Health data processing - system theory based meaning and potential for future health. In Doucek, P., Chroust, G., and Oskrdal, V. (eds), IDIMT-2015, Information Technology and Society - Interaction and Interdependence, pages 423–430. Trauner Verlag Linz, Sept. 2015.

[3] Aumayr, G., Chroust, G., Haider, G., Randus, R. & Thür, A. (2015). Disaster- management: challenges for computer-supported process and project management. In Ison, R. (ed),

Governing the Anthropocene: The greatest challenge for systems thinking in practice? - Program and Abstracts, pp. 107-109. ISSS, International Society for Systems Sciences, 2015.

[4] Azuma, R. (2004). Overview of augmented reality. In SIGGRAPH ’04: ACM SIGGRAPH 2004 Course Notes, pp.26, New York, NY, USA.

[5] Backfried, G., Göllner, J., Quirchmayr, G. et al. (2013). Integration of media sources for situation analysis in the different phases of disaster management. In EISIC 2013, IEEE, University of Upsalla, SWE.

[6] Bolin, R. & Standford, L. (1998). The Northridge Earthquake: Vulnerability and Disaster. Routledge, London 1998.

[7] Brose, D. (2015). Developing a framework for measuring community resilience: summary of a workshop. The National Academies Press 2015. Available via http://www.nap.edu/catalog.php?record_id=20672.

[8] Bundesamt f. Bevölkerungsschutz und Katastrophenhilfe (2011). Psychosoziales Krisenmanagement in CBRN-Lagen / Psychosocial Crisis Management in CBRN Incidents. Bundesamt f. Bevölkerungsschutz und Katastrophenhilfe, Germany 2011.

[9] Chroust, G. & Aumayr, G. (2015). Resilience 2.0: ICT for Resilience of Systems. In Doucek, P., Chroust, G. and Oskrdal, V. (eds), IDIMT-2015, Information Technology and Society - Interaction and Interdependence, pp. 13-22. Trauner Verlag Linz, Sept. 2015.

[10] Chroust, G., Ossimitz, G., Roth, M., Sturm, N. & Ziehesberger, P. (2015). First responders in regional disasters: a social responsibility. In Mulej, M. and Dyck, R. (eds), Social Responsibility - Range of Perspectives per topic and Countries, pp.23. Bentham Science Publishing Ltd., 2015.

[11] Chroust, G., Schönhacker, S., Rainer, K., Roth, M. & Ziehesberger, P. (2009a). Dependable systems, emergency interventions, and organizational processes. In Doucek, P., Chroust, G., and Oskrdal, V. (eds), IDIMT 2009 – System and Humans - A Complex Relationship, pp.279-287. Trauner Verlag Linz, 2009.

[12] Chroust, G., Schönhacker, S., Rainer, K., Roth, M. & Ziehesberger, P. (2009b). Training and supporting first responders by mixed reality environments. In 53rd Annual Conference - The International Society for the Systems Sciences " Making Livable, Sustainable Systems Unremarkable", pp.18. The International Society for the Systems Sciences 2009 (CDROM), July 2009, paper no. 2009-1248-Chroust.

[13] Chroust, G., Sturm, N., Roth, M. & Ziehesberger, P. (2011). Regional disasters and systemic reactions. In Wilby, J. (ed), ISSS 2011 and ISKSS 2011: All Together Now: Working across Disciplines, pp.15 (paper no. 1631). (CDROM) Int. Systems Science Society, UK, 2011.

[14] Cruz, A. M. (2005). Natech disasters: a review of practices, lessons learned and future research needs. Technical report, available via ipcc-wg2.gov/njlite_download.php?id=6152 [Dec.2014].

[15] Diamond, J. (2005). Collapse - How Societies Choose to Fail or Succeed.

Penguin Books London, 2005.

[16]Dörner, D. (1996). Die Logik des Misslingens - Strategisches Denken in komplexen Situationen. sachbuch-9314, rororo Verlag, Hamburg.

[17] Filippoupolitis, A., Hey, L., Loukas, G., Gelenbe, E. & Timotheou, S. (2008). Emergency response simulation using wireless sensor networks. In Ambi-Sys '08: Proceedings of the 1st International Conference on Ambient Media and Systems, pp.1-7, ICST, Brussels, Belgium. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[18]Francois, C. (2004). International Encyclopedia of Systems and Cybernetics. 2nd edition, 2 volumes, K.G.Saur, München 2004.

[19] Greengard, S. (2014). Weathering a new era of Big Data. Comm. ACM, 57 (9): 12-14.

[20] Grifantini, K. (2009). Can you trust crowd wisdom? Technology review (MIT), Sept. 16, 2009.

[21] Haddow, K. & Haddow, G. (2008). Disaster Communications in a Changing Media World. Butterworth-Heinemann Homeland Security, kindle-book, 2009.

[22]Holling, C. (1986). The resilience and stability of ecosystems. In Clark, W. and Munn, R. (eds), Sustainable Development of the Biosphere. Cambridge Univ. Press 1986.

[23] IFRC (ed.) (2007a). Contingency Planning Guide. Technical report, International Federation of Red Cross and Red Crescent Societies, 2007.

[24] IFRC (ed.) (2007b). Disaster Response and Contingency Planning Guide. Technical report, International Federation of Red Cross and Red Crescent Societies, 2007.

[25]INSARAG (ed.) (2012). INSARAG Guidelines and Methodology Technical Report. Technical report, International Search and Rescue Advisory Group, United Nations Office for the Coordination of Humanitarian Affaires, 2012.

[26]ISO (2011). ISO 22320:2011, Societal security – emergency management – requirements for incident response. Technical report, International Organization for Standardization, 2011.

[27] Kelton, D., Sadowski, R. P. & Sturrock, D. (2007). Simulation with ARENA. McGrawHill, Boston 2007.

[28] Khan, H., Vasilescu, L. & Khan, A. (2008). Disaster management cycle - a theoretical approach. Management and Marketing Journal, 6(1): 43-50.

[29] Kreps, G. et al. (1989). Social Structure and Disaster. University of Delaware Press, Newark, 1989.

[30] Lazarte, M. (2013). New ISO standard for emergency management. Available via http://www.iso.org/iso/home/news_index/ news_archive/news.htm?refid=Ref1496, [Feb. 2014].

[31]Manahl, C. & Drechsler, F. (2015). Engaging end-users in the development of smartphone applications for emergency services. In Doucek, P., Chroust, G. & Oskrdal, V. (eds), IDIMT-2015, Information Technology and Society -Interaction and Interdependence, pp.39-44. Trauner Verlag Linz, Sept. 2015.

[32] McEntire, D. (2007). Disaster Response and Recovery: Strategies and Tactics for

Resilience. Wiley, USA 2007.

[33] Mrotzek, M. (2009). Catastrophe dynamics - a systemistic exploration of catastrophes towards a set of catastrophe archetypes using the system dynamics simulation method. PhD thesis, Faculty for Technical Sciences, Alpe-Adria University Klagenfurt, Feb. 2009.

[34] Mrotzek, M. & Ossimitz, G. (2008a). Catastrophe archetypes - using system dynamics to build an integrated systemic theory of catastrophes. In Chroust, G., Doucek, P. & Klas, J. (eds), IDIMT-2008 - Managing the Unmanageable, 16th Interdisciplinary Information Management Talks, pp. 371-384. Verlag Trauner Linz, 2008.

[35] Mrotzek, M. & Ossimitz, G. (2008b). An integrative systemic theory of catastrophes - Studie für KIRAS nr. 813798 proj. SimRad.NBC. Technical report, Inst. f. Mathematik, Univ. Klagenfurt.

[36] Norris, F., Friedman, M. & Watson, P. (2002). 60.000 disaster victims speak: Part ii.: summary and implications of the disaster mental health research. Interpersonal & Biological Processes, 65: 240-260.

[37]Ossimitz, G. & Lapp, C. (2006). Katastrophen - systemisch betrachtet. Wissenschaft & Umwelt 2006 – INTERDISZIPLINÄR, 10: 51-62.

[38]Pfahl, D. (2005). System dynamics simulation - a tool in support of software risk assessment and decision support. Tutorial at IASTED SE 2005, Innsbruck, Austria, February 17, 2005, Handout.

[39]PublicSafety.NET (2015). For further development of broadband services in disaster relief - whitepaper. Available via http://www.johanniter.at/forschung/D81whitepaper.pdf [January 2016].

[40]Quarantelli, E. (1985). The need for clarification in definition and conceptualization in research. In Sowder, B. (ed), Disasters and Mental Health - Selected Contemporary Perspectives, pp. 41-73.

[41] Roth, M. et al. (2012). SIMRAD.COMP: Simulations- und Informationssystem zum Administrieren von Hilfseinheiten bei Katastrophen - Erforschung von Systemkomponenten zur Überprüfung der Einsatztauglichkeit der SIMRAD Technologie, Endbericht Projekt KIRAS 818784. Technical report, Österr. Forschungsförderungsgesellschaft mbH (FFG) 2012.

[42] SimRad.NBC (2009). The SimRad.NBC - simulation- and information system to manage rescue units at disasters – with focus on NBC threats. Available via http://www.simrad.at [May 2009].

[43] Skrbek, J. & Kviz, J. (2010). Critical areas of early warning system. In Doucek, P., Chroust, G. & Oskrdal, V. (eds), IDIMT 2010 Information Technology - Human Values, Innovation and Economy, Sept 2010, pp. 193-200. Trauner Verlag Linz, 2010.

[44] Svata, V. (2012). ICT Methodological support of disaster management. In Doucek, P., Chroust, G. & Oskrdal, V. (eds), IDIMT 2012 - ICT Support for Complex Systems, Sept 2012. Trauner Verlag Linz.

[45] Taleb, N. (2012). Antifragile: How to Live in a World We Don’t Understand. Penguin UK 2012.

[46] Tierney, K., Lindell, M. & Perry, R. (2001).

Facing the Unexpected - Disaster Preparedness and Response in the United States. Josef Henry Press, Washington DC, SA 2001.

[47] Wikipedia-english (2013). Wikipedia, the free encyclopedia. Available via http://en.wikipedia.org/wiki/.

Gerhard Chroust is an Austrian systems scientist and Professor Emeritus for systems engineering and automation at the Johannes Kepler University of Linz, Austria. He is the Secretary General of the International Federation for Systems Research (IFSR) and a Board Member of the Austrian Computer Society (OCG). He is an Honorary Member of the Austrian Society for Informatics (ÖGI) and of the Bertalanffy Center for Study of Systems Sciences (BCSSS). Chroust is an authority on formal definition of programming languages, system development processes, software quality standards, process assessment, and on cultural differences in system development. His current key research is in human aspects, cultural differences and systemic aspects of system development and disaster management, and representation and enactment of software processes. In 1964 he received a Master of Science (electrical engineering) from the Technical University, 1965 a Master of Science (computer science) from the University of Pennsylvania. In 1975 he was awarded a PhD (computer science) from the Technical University Vienna and in 1980 a Habilitation (Computer Science) from the Johannes Kepler University Linz. From 1966 to 1991 Chroust worked at the IBM Laboratory Vienna. From 1992 until 2007 he was tenured Professor for 'Systems Engineering and Automation' at the Kepler University of Linz. He has published 10 authored books, edited/co-edited approx. 60 proceedings, written approx. 220 scientific publications and approx. 300 other publications. Chroust is bearer of the Silver Medal of Honor of Upper Austria. Website: http://www.gerhard-chroust.at.

Georg Aumayr is an Austrian health promotion and communication scientist. He received his Master in Communication Science at the University of Vienna in 2007. Aumayr is head of the research and innovation center of Johanniter in Vienna, Austria and the research officer of Johanniter International in Brussels, Belgium. During large scale events like the EURO2008 he worked as EMT and was active ambulance staff and first aid instructor for several years. Aumayr worked also for the pharma industry in marketing and ICT as well as for the University of Vienna as assistant. He was from 2010-2012 member of advisory groups for Ambient Assisted Living and Emergency Care in Austria as well as Evaluator for European Research Programs. Since 2010 he is constantly engaged in European research projects and national research projects in the area of health promotion and ambient assisted living as well as in disaster relief from situation awareness systems to personal protective equipment. His current key research is the promotion of health under extreme or constantly changing situations like in disasters or at the process of ageing.