SecInCoRe

Co-Design Workshop I
Manchester
9-10 December 2014

Workshop Report Advance Copy

Objectives

Understand	current practices of emergency responders of various roles
Envision	technological potential and its relation to practice
Experiment	with new ways of working that integrate new technologies
Collaborate	professional experts, social scientists and engineers

Co-Designing Crisis Response Futures

The 21st Century has been labeled 'the century of disasters. More disasters and heightened vulnerability shape a 'new reality' for the emergency services. There is a need to increase efficiency, interoperability and coordination with a less experienced but more technology-savvy workforce.

Technology is often championed as a solution. However, benefits from technological potential can be hard to realise.

Collaborative Design (Co-Design) is an approach that brings professional experts, researchers, and designers together to align users needs, technological potentials, and professional practices to develop novel and unforeseen solutions. It is motivated by the fact that practitioners must be able to use new technologies effectively, creatively and in line with their professional practices. To maximise benefits, to notice and address risks requires grounding innovation in understanding of current practices and emergent new ways of working.

Understanding Information Flows

Response experts listed over 40 different data types, ranging from weather reports to information about the topography and affected populations to location of resource. Over 20 different data sources are regularly drawn upon, including local authorities, historical records, and utility companies.

Unity in Diversity

"The job's the same, but there are many ways of doing it"

Bringing together response experts from seven different countries brought home how important it is to attend to similarities and differences in:

- Emergency Response Processes and Roles
- Data sets
- Information Systems
- Business Models
- Ethical, Legal and Societal Frameworks for Emergency Service provision
- Languages!

Even if standardisation progresses, diversity will remain an integral feature in practice, especially when transnational collaboration is needed.

Linguistic and conceptual 'translation' is needed to support coordination across different frameworks.

But diversity matters even at national levels, where mechanisms such as Local Resilience Forums can be a platform for coordination.

A taxonomy should support translation between roles, languages, IT systems, etc. to make a pan-European disaster inventory and a common information space useful. But …

"It's not just about sharing the information / data – it also needs to be needed & understood by the recipients."

Diverse needs and perspectives shape how data e.g. on 'people affected' is sought:.

Vulnerable people requiring specialist assistance
People whose presence is not compatible with rest-centers
People at risk
People needing evacuation
Number of victims
Survivor/fatality information
People with disabilities
Anyone needing to be rescued?
Anyone still missing?
Location of people at risk
Trapped people?

Instead of translating all these to one data type, the goal should be to offer a structure that models the differences while helping them talk to each other.

Keep IT simple, Keep IT safe

"If mains electricity is absent, we are battery dependent"

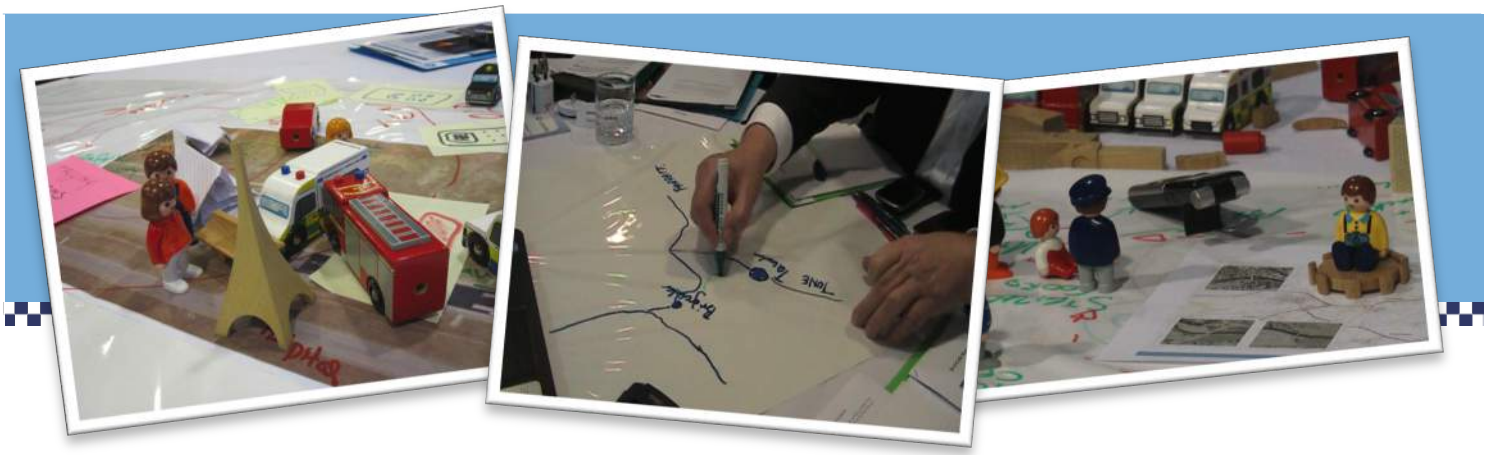
Technology is of no use if people cannot use it effectively and creatively or it creates additional risks. Questions included:

How will the inventory be populated and whose responsibility is it to **keep data accurate and up-to-date**? How will this be done?

If technology requires additional work – who will do it and when?

Whilst calling to keep IT simple, people also revealed that they use many complex technologies in complex ways. **Does 'simple' actually mean 'familiar'** and does this mean all IT should be in everyday use?

And sometimes simple things can get in the way – technology depends on power and some areas may be restricted to 'intrinsically safe' devices.



Information Is Not Enough

"It's a question of how you use what is available that is important. Just because you *can* run video doesn't necessarily mean you need to *do* it."

More information will not solve information problems, even if there are new sources. New information requires **new techniques for collecting, sharing, analysing**, and can create clutter in an already overwhelming situation.

Tools are needed that can aid in the activities and decisions that are needed to make and make sense of information.

For example, one response expert discussed the value of incorporating volunteer data to expand situation awareness, yet:

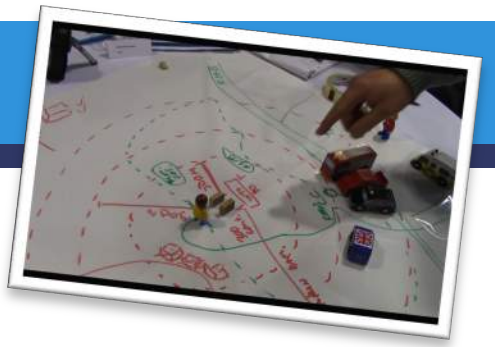
"If you're all high tech, all integrated with mapping people on GPS and somebody rings in and reports I'm walking up the road, how do you inject such 'low tech' reports onto your displays?"

New technology to integrate more information also leads to difficulties with different agencies' capacities in accessing, processing data, and prioritizing the often-conflicting data. More can mean less for some.

Sandboxing real world experience showed how in response to a large area flood, responders used aerial photographs of bridges made impassable. This was pivotal, but it was impossible to share the high resolution images between all agencies along a complex command chain.

And, as experts described the uncertainties of incidents, it also became clear that some data is–and always will be–unknown regardless of the available technology and the amount of data collected.

Sandboxing Incidents: Learning from real experience



A: *Was it safe to make the hole? No. That's why the town was evacuated.*
Q: So there was no data about what the container contains?
A: Not exact [data], no.

When responders in Finland were called to a smoking container, the uncertainty about the precise nature of the chemicals inside prompted them to evacuate a nearby town and drill a hole to test its contents. Lessons learnt include:

- Don't under-estimate the amount of data which could be made available to share.
- **'Collect all' is not the answer.**
- There will always be a need for more information

SecInCoRe should develop tools that support people in noticing, determining, and improving the **quality, including relevance, appropriateness, timeliness, and compatibility** of information.

Information Management

The question is not just how to support **more information sharing** in a **networked common information space**. People sometimes don't share because they **don't want to share**, or because they can't or because they cannot make sense of the information.

'We need to know the **when, where, and why** of information to **draw the line**, to **manage information** and to decide **who is kept out**.'

It was quickly evident that managing information flows should be a central focus of any useful information system, not just managing the production of information from data. The response experts argued that the greater the circle of actors in any information sharing system, the greater the need to delimit accessibility and to guarantee added value for the different roles and responsibilities.

Data Perimeters

Managing who should know what and in what way.

As SecInCoRe identifies a wide range of data sets to incorporate into a information space, one aim is to facilitate the inclusion of new, yet vital, data sets and sources. This would bring into view the wider spectrum of people often involved in disaster responses. The idea was welcomed by the response experts, who said we should:

"look at how, in effect, information can be drawn from crowdsourcing sources like that, draw information from twitter... though not an authoritative source, actually say it's there to inform people."

But such enthusiasm came with caveats. Inclusion and accessibility of a wider range of data and sources means greater needs for management. Sharing everything with everyone is both a problem of clogging the communication lines, and of differentiating signal from noise. This invites an ethical question: if you take data from NGOs or the public, do you have to share back? Sharing with these groups can be problematic for another reason:

"We can't fight fires and have everything go back into the public, because it comes back to ethics: if you make the decision to sacrifice someone's property for the greater good and someone puts that out in the public domain, then its going to get back, and then you are suddenly the target because the decision you made."

One effect of increasing the range of data sources is a need to create clearer rules for data perimeters. It starts with two questions: How far down the response chain does data need to go? How broad in range does the data need to be? It also involves managing on multiple planes of information sharing at once: sharing between strategic and tactical sections, sharing between agencies or with private companies, sharing in different phases of crisis management, managing public understanding, media messages, and social media trends.

Scalability

Sharing needs to be a scalable process spatially and temporally, so that it can basic enough to be part of daily practice yet durable enough to work on international responses. To work, SecInCoRe needs to design something, be it a technology or an organisational system, that considers everyday incidents and infrequent ones, the small and the large, the routine and the exceptional.

Virtuous Technology: Ethical, Legal, and Social Issues

data security
people security
information management
liability
misinformation
accuracy
rights to data
obligation for safety
public understanding of data access
managing the 'unpopular'
sovereignty
inclusiveness
impartiality
trust
preparedness
transparency
visibility
vulnerability

"The legislation hasn't kept up with the technology."

"Are you fighting the scenario or are you fighting the technology?"

Useful Technology

There was no agreement in the group as to where the user ended and the technology began in relation to information failures. While all agreed that technology should be made to be familiar and used everyday, they disd not agree on what solutions could be technological and which based on practices. Conversations like this were frequent:

R1: What happened in Schiphol with the air crash, they used TETRA which was designed as an emergency response tool and it failed because of design not technology.

R2: No it's not TETRA that failed, it's users that failed, because they are not using it well.

One of the response experts summed it up well when he stated:

"Are you fighting the scenario or are you fighting the technology?"

These issues were exemplified by a constant referral to the failures of TETRA. TETRA was a common denominator in the discussion, being one of the most widespread technologies. But it became clear that no two groups used it the same way, and no one thought it was used well, despite its potential. Procurement did not involve the users and this, according to one responder, "meant there were limitations in how the system was used." Involving users is vital to technological success.

Transparency

For a technology to be useful, it must provide various forms of transparencies, such as being transparent towards the public and balancing the right to the data with the most useful data needed for the situation. Discussion revelaed further, more subtle, yet equally important, forms of transparency.

The technological system needs to provide information about the data in such a way that in enables decisions regarding the relevance, usefulness and effects of using that data in this way. For instance, could a high quality still image include with it how often it arrives, its bandwidth needs, and how it affects the communication pathways were it to be shared? Effects of using technologies in particular ways need to be made transparent. TETRA can be used for 1:1 communications, but if you are using it in that way it can clog the system. Security should also be transparent, especially when engaging with organizations outside formal response, to increase trust in these interactions.

From Participants

We have received many **extremely helpful comments** from participants during and after the workshop. On this page we present a selection to give you a feel for the kinds of insights produced – there is much more we will be working with!

Interoperability: Holy Grail?

We can share it but do we want to?

In the Army, I worked in an Engineer Regiment that formed part of NATOs' Northern Army Group. **Every year, the Engineer units in this Group came together to discuss the formalisation of interoperability.** I attended the 40th annual meeting of this group and it was apparent that even in the face of an overwhelming opponent, **there was very limited 'will' to enhance interoperability or agree common procedures.** This will doubtless be an issue that you will face as your project proceeds.

It's easy to decide who can access what when all information is known. When information is being gathered it's less easy.

Digital Divides

The haves and have-nots

There will be an issue with the introduction of enhanced technology over the interface with organisations that do not have access to the same technology. This might create distinct splits within a response between the haves and have-nots as well as creating difficulties in coordination of the response.

Sharing as Cyclic

Avoiding dead-end pathways

Sharing needs to be a cyclic process and long-term, not something which just takes place during an incident:

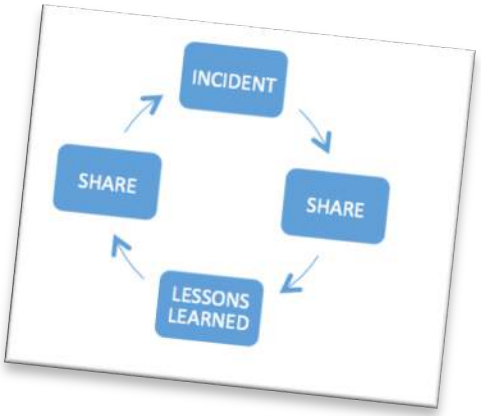
Experience suggests that organisations may initially embrace interoperability and common processes but, over time following implementation, **internal pressures and cultural differences** between organisations will lead to reduced engagement of individual organisations and divergence from agreed processes.

Thinking About Capabilities or Technologies?

Is this really a technology problem or is the reality more to do with obstacles such as parochialism, politics, governance etc.?

This question, key to our project, relates directly to changes in how the responders refer to their information sharing:

Increasingly **we refer to capabilities rather than equipment or resources.** This is important as a list of equipment or resources may be misleading.



This change in discourse and focus addresses the fact that:

Some failures in information exchange or lacking information during a disaster event are **very difficult to be closed with more technology.**

Sometimes equipment does matter

Everything we use needs electricity in some form – mains or batteries.

More Workshop Results

- Evaluated SecInCoRe's ideas so far
- Co-designed a vision of a socio-technical 'product'
- Translated ideas across the boundaries of academia, design and practice
- Gathered information as to the opportunities and challenges users see in interoperability and information sharing
    - Explored important debates regarding how to address user needs
    - Assembled materials (case studies and technologies for collaboration)
    - Developed a methodology for encouraging ethical co-design
    - Identified a set of people to work with more long term

Key Questions

How can we anticipate emergent future practices and socio-economic contexts in the design of systems and in organizational innovation?

Should the focus be on the areas of convergence or the areas of difference?

Can and should the inventory be used during an active response?

How should stakeholders outside of the emergency services be brought into a common information space?

What kind of security is needed as data travels between different sources?

What still needs to remain face-to-face interactions?

How do you build a system that is transparent while simultaneously supporting difficult decision-making?

Who will maintain the data repository?

How do you build into the system support for awareness of ethical, legal, and social issues data practices?

How to support people in determining appropriate data quality, accuracy, reliability in different circumstances?

Next Steps

Continue discussion about basic concepts, such as Common information space, inventory, networks.

Follow up with in-depth interviews and future workshops.

Develop publications based on our results, especially ones that focus on the value of co-designing **with** users and stakeholders not just for them.

Work creatively and proactively with the fact that we are designing technological tools, specifications, organizational practices, and social-technical futures.

Use the results from this workshop to develop **new and useful technologies and organizational innovation** that supports human practices of unity in diversity, translation, collaboration, information management, simplicity, familiarity, creativity.

Stay in touch.