SecInCoRe

Co-Design Workshop II
Athens, 10-11 September 2015

Report

Hard to achieve, but what I want

"… it may be a goal, especially on a European level that can't be achieved. But it's just what I would want, maybe not next year but in ten years time."

SecInCoRe explores how an inventory of past disasters could serve as a basis for a networked 'common information space' for emergency management.

This report reflects upon insights from a co-design workshop that brought together 16 emergency service practitioners, including responders, planners, and legal professionals, and the interdisciplinary SecInCoRe team. The aim of the workshop was to envision, experiment with and evaluate SecInCoRe concepts. Activities took departure in a 'case study' of the migration/refugee crisis unfolding in Europe.

Participants quickly found a consensus that an inventory of data sets, 'lessons learnt', crisis management models, and a common information space to facilitate mutual learning and coordination would be useful.

However, the complexities of realising and putting these concepts into use, and with pan-European ambitions to boot, gave rise to lively debate. The pan-European scope, the complexities of networking and sharing, and the idea of a 'common information space' in particular attracted much discussion.

The project does not aim to design a technological solution 'for tomorrow' but a concept that integrates technological, organisational, and policy innovation with a more long-term view. This makes it difficult to reconcile the concrete demands of practice with the vision. One practitioner summed up the challenge perfectly:

Going 'step by step' would be a very practical response but being a proof of concept we should be looking at the ideal, the ultimate - getting there is always going to be a journey, […] we need to look at the big picture …

Objectives

Experiment

with new ways of working

Collaborate

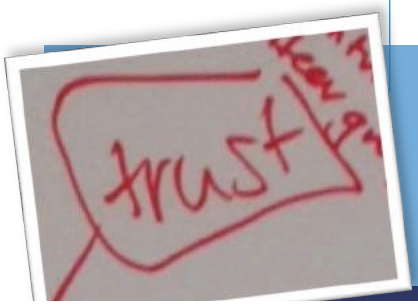
professional experts, social scientists and engineers

Envision

creative responses
design trajectories
organisational practices

Evaluate

technologies, practices, policies, concepts, ideas



Trust in information | people | organisations

Trust is key to good collaboration. It is not a static quality, but a dynamic effect of interaction with information, people, organisations. It is achieved in specific situations. **Key Insight:** Don't replace but ***augment*** emerging practices of trust***ing***, such as communicating with people you know.

A pan-European concept?

"It's a massive undertaking to achieve something across an EU level that no countries have achieved yet (at a national level)"

There was much discussion about the challenges of developing a pan-European concept. Some practitioners felt that we should start small, perhaps at a national level, and with 'a core group or core country' to make sure the scope was manageable.

At the same time, there is a need to think big:

"It's not a good solution to have it European but it's the only solution …, otherwise you don't get the information you really want"

Make IT concrete

SecInCoRe needs to do both: make change managable and 'think big'. Its inventory already compiles nationally specific as well as pan-European case studies and should ultimately map information resources across the EU.

By developing a concrete 'proof of concept' 'demonstrator' or prototype that utilises the inventory to support construction of common information spaces, SecInCoRe can – in the next phase of the project – facilitate experimentation with national and pan-European collaborations.

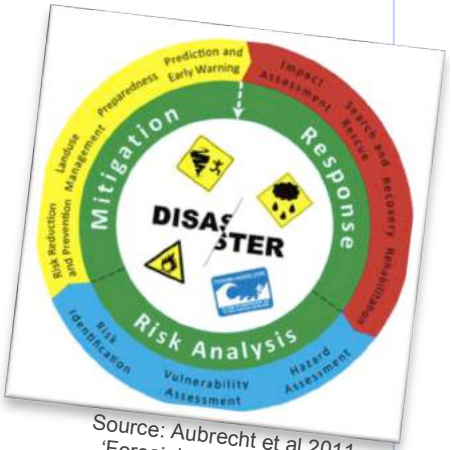
Would you SecInCoRe during a Crisis?

SecInCoRe has been conceived of as a concept that will support diverse stakeholders in dealing with disasters. But when? And how? Is it to be used during response, and as a decision making tool? Or will it be used mainly for planning and training?

Discussions revealed significant differences, for example in levels of authorisation and access to information, which may change between strategic planning and operational phases.

But there are also overlaps. The refugee/migration crisis illustrates how response, risk analysis, planning and mitigation can blur and how, even within the response phase of a major crisis, as it unfolds over time, there may be occasion for SecInCoRe supported information work and collaboration.

Discussions enriched understanding of the crisis management cycle or spiral.



Source: Aubrecht et al 2011 'Foresight and Prediction'

BRIDGE Project Master Concept
http://www.bridgeproject.eu/en

Shaping a Common Information Space

There are many examples of common information spaces (CIS), ranging from the Japanese 'resilient society' integration of public databases to Rio's smart city control room, to the UK's 'Resilience Extranet' or the BRIDGE project's 'Master'.

The SecInCoRe workshop demonstrated that ideas of how a CIS might work in practice vary widely. In order to develop the SecInCoRe CIS concept, we explored how practitioners might contribute to and how they might retrieve information from a common system.

A specific set of requirements is starting to emerge from this, highlighting that a CIS should support secure sharing as well as discovery of differences in structures and interpretation, relationships between different types and sets of data. It should enable communictaion, negotiation and translation.

It is important that a CIS is not a data 'pool' where all users 'upload' content for all to access equally.

Instead, it should be a networked environment where participants who are distributed in space can discuss information appropriate to their role and the respective context, where they can be aware of what others know or need to know, and how they understand it.

Trust is a matter of trust*ing*

"If I phone with rank and organisation you get one bit of information, but if I met you around the table you'll get more information because of trust. You can't build that into the system so the system gets the lowest common denominator"

In numerous descriptions like these, the practitioners pointed out that trust is an interpersonal and situated achievement and key to successful cooperation.

Its central role must recognised in the design of SecInCoRe. If it cannot be 'built in', it must be supported in other ways.

By discussing how trust is achieved in practice, the workshop participants began to explore the design of SecInCoRe concepts that can support practices of trusting.

Practitioners reported that having trust in information often starts with knowing where it had come from or who was the source:

> *If it's from a credible source we've used many times … we'll say right, we'll trust anything that person says*

For many people a credible source means an official agency or public organisation, but it could also mean a person one had an established relationship with or whose reputation had been confirmed.

Making sources inspectable and utilising existing accredidation and reputation mechanisms are thus useful techniques. A 'LinkedIn'-type map of social connections may also be useful.

A range of further suggestions for support arose, including:

- Ways of finding out who to talk with about specific issues for more information
- Contact lists that aren't individual but role-based
- Employing information validation standards, such as a 'Four eyes' process
- Restricting membership to first responders or making it possible to engage only with similar agencies
- Providing tools to help see how unfamiliar roles or information from a new context could be relevant

Trust in information, people, organisations must be underpinned by trust in systems.

In a cloud-based information space, where would the data be located and how can each country and each organisation access them securely?

A harmonisation of the different law frameworks across the EU would be a way to address the problem, which might fall outside the scope of SecInCoRe but it indicates that policy pressure should be applied in that direction.

IT's all about Communication

> *You either know someone or someone that knows someone and try to get relevant information.*

This dependence on social relationships and networks makes pan-European cooperation difficult.

Talking to someone, even in the same agency in a different country was often *'unbelievably difficult'*, partly because there are different terms and structures.

It can be a challenge to even work out '*what is the question*'.

This is about more than trust.

For instance, when responders wanted to learn from others who had set up a distribution centre, they said:

> *it's better if you came rather than just talking on the phone…look at our distribution centre, see how we run it.*

Words, numbers, procedures become meaningful in context.

While SecInCore cannot replace face-to-face and 'face-to-place' contact, it can support people in contextualising data, e.g. by:

- Providing up-to-date pan-European contact details
- Translating and mapping roles across different national cultures and languages
- Enabling multiple secure multi-media communication channels
- Developing 'who or what am I missing' visualisations of other people's networks

Case Study: The Migration/Refugee Crisis

The migrant/refugee crisis unfolding at the crossroads of Middle East, Africa and Europe proved an interesting focus. It was chosen as a 'case study of case studies' to test the design of the SeInCoRe inventory of past disasters, and as a basis for exploring the use of SecInCoRe Common Information Space concepts.

It also allowed us to to get a more detailed picture of how this pan-European crisis is being framed and dealt with in different regions and by different organisations. This page summarises some of the main insights.

A Disaster or Business As Usual?

There was a surprising range of stances among the practitioners on how the situation should be understood, framed and ultimately managed, highlighting the relationship between the political and the operational.

While some practitioners, especially those who work in reception countries such as Greece and Italy spoke about an urgent disaster which unfolds in an almost uncontrollable way and about their operational struggles to manage the situation, others felt '*well removed from the situation'* and asked '*is this a crisis or just a lot of work*'?

Rethinking borders, boundaries and terms

The disparity of views sparked further debates such as what makes a crisis, or a disaster and when does a crisis start or end, whether this is a new situation or part of the long phenomenon of immigration, but also the question whether there was the political will to recognise it as a pan-European crisis that needs a joint approach, a configuration of national or local disasters, or even a global crisis that involves non-EU countries instrumental in the response and planning (such as Turkey or third-country embassies). Understanding these nuances is important for SecInCoRe in order to properly support and enhance mutually respectful and productive collaborations.

Differences often also emerged about what the issues at the center of this crisis actually were. For example, in reception countries, the police focus on distinguishing between legal refugees and illegal migrants, a practice necessary for the registration process. This is important because 'intelligence' issues raised could be mobilised to avert greater crisis. In other areas, however, first responders and organisations such as the Red Cross, did not see such classifications of people as significant. This is because for them, the situation is a humanitarian concern rather than a security issue. As one practitioner put it *'as first contact responders, our job is to look after people*'.

Syrian refugees strike at the platform of Budapest Keleti railway station. 4 September 2015, by Mstyslav Chernov, available from Wikimedia Commons http://tinyurl.com/ncjqtn5

Lessons Learned

The practitioners generally agreed that pan-European coordination enabled by a concept like SecinCoRe was needed. There is a need to cope with significant differences in using data with regard to organization types (fire departments, medical services, police or Search & Rescue), as well as countries and political situations.

One benefit from a pan-European inventory could be sharing of good practices and educational content. Even though for some types of organisations or countries the crisis is not a kind of emergency yet, this might soon change. Many of the participants from EU countries other than Italy and Greece are experiencing demand on emergency services and emergency planning to respond to the movement and needs of the refugees and migrants. This supports the idea of an inventory, and of making information available before it is actually needed to be prepared.

Engagement with Diverse Stakeholders

Spontaneous volunteers

Spontaneous volunteers emerged as a significant issue for some practitioners, often in the context of how to plan for or manage such volunteers, as well liability, insurance and legal issues.

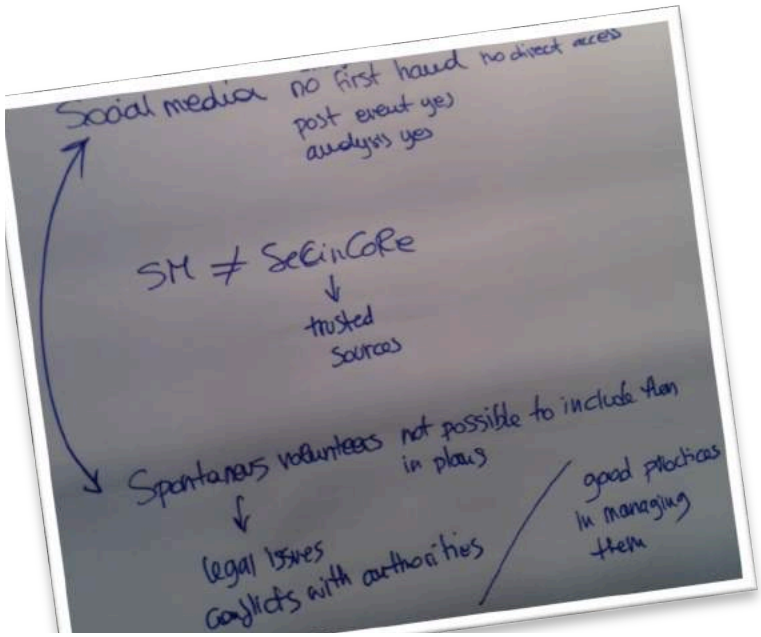
Some practitioners saw a role for SecInCoRe in helping to gather best practice examples and lessons learnt for how to work with spontaneous volunteers.

However, there were also serious concerns about including such groups in a SecInCoRe Common Information Space:

> *If it is just for professional organisations then [we] know information is valid [but if we were] allowed to have spontaneous volunteer groups? That would make things difficult.*

This perspective, in turn, was challenged:

> *The question is exactly the other way around. Why are we not able at the moment to manage that and is there an information platform that may be helpful? Cause to be honest […] we don't know […] which needs we have from spontaneous volunteers […] what offers they are making.*



Social media

Engaging with social media also involved tensions:

> *On one hand you need researchers always scanning social media for new information. On the other it's a question of liability.*

Practitioners agreed that it was vital to be in tune with how the public were responding to a crisis and that it was 'wrong' not to be aware of people's communications on social media as that could be where initial reporting comes from. However, discussions also revealed major concerns about including social media contributions in SecInCoRe. For some it was not in the remit:

> *The question of using social media is just a completely different field to the objective of SecInCoRe.*

Other concerns centred around trust, accuracy and not knowing the source. One practitioner had seen hesitancy at a local level, where services used social media to share information, but not as a source:

> *There's been a great reluctance for coming the other way, I guess you build up trust in people that you know.*

Some thoughts

Which stakeholders we see as part of SecInCoRe is influenced by how we define security. Is security something to be 'provided' by first responders to passive publics or a wider social and political responsibility that always involves citizens?

In either case, SecInCoRe is not a hermetically sealed system, where those tasked with security can freely and securely share information once they are 'in'. Instead, it uses an inventory portal to an already networked universe of information systems (including social media platforms) and provides stratified access defined by access rights and responsibilities.

As such social media data sets and actors are 'in'. But the question remains how formal and informal response can engage with each other given their different approaches and their stratified access within the common information space.

Access & Security

"Should it be fixed agencies or emergent and new partners? You wouldn't want to exclude people but maybe have a system of accreditation so don't prevent people but have an access level."

The question of who should have access to use and contribute to SecInCoRe was central to many discussions. Practitioners stressed that confidentiality and data integrity were key to the integrity and success of the concept.

Thus the question of what kind of access stakeholders such as the public, the media, volunteer groups, or even NGOs should have was of great concern.

On the one hand, some practitioners felt strongly that

> *authorisation to access information in the system has to be restricted*

Allowing official agencies only was a preferred solution for some.

Others saw value in having a system that could allow new partners to access the system quickly if needed since:

> *You might need partners you never thought of.*

However, they felt such an option would require authentication processes.

A stratified system that differentiates between open, restricted, and classified information would offer different clearance levels for accessing information.

Such a system could offer an open basic level of access that would accommodate public contributions and the crowdsourcing of information, while at the same time reserving higher levels of access for professionals and institutions.

SecInCoRe is developing support for such stratified access, including chip and PIN, a public key infrastructure, and digital signatures.

Discussions highlighted that the stratification mechanisms would have to be dynamic, as different roles are involved in different ways and have differing responsibilities and hence different levels of authorisation in different incidents.

Moreover, security of access must be finely balanced with ease of use and clear functionality.

SecInCoRe certainly faces challenges here!

Sensitive data, privacy and data protection

Source: Digitaldemocracy http://tinyurl.com/nv5f2tw

Challenges of privacy, data protection and security manifest differently in different phases.

During response, exceptional exemptions may allow sharing that would otherwise be prohibited, while, in times of planning, practitioners explained that different data sets would be used, shifting away from personal data towards more aggregated data sets and statistical data.

However, data may still be sensitive:

Risk plans can include confidential information (such as infrastructure maps) and incident reports include personal data about responders as well as sensitive information. Debriefing reports also often include information about *why* something was done, which can come under scrutiny in public enquiries that seek to apportion liability with hindsight.

Most organisations have strict information security policies.

SecInCoRe should support stratification of data access according to context to allow people to transpose such policies into common information spaces.

This also raises issues of data location, as already discussed under the heading of Trust.

Creating 'added value'

For people to use the SecInCoRe inventory and CIS they must facilitate the production of 'added value'. Suggestions included:

Having a contacts database

Some sort of contact mapping was seen as a valuable addition. This could include what organisations were responsible for what in different countries along with their contact details. It might also mean having 'who' to contact for further information about a particular document.

Presenting enriched data

Extending the range of information that can be considered, could also mean finding new links among data, suggestions for other information and searching by keyword. This could add context to data.

Mapping of existing databases

There are many different information sources and databases across Europe. Something that maps and provides links to different information sources would be an asset.

Resources for learning & training

The ability to learn from others was seen as a key benefit of a concept like SecInCoRe.

This included learning from other's experiences through information exchange; learning from past events and having a source for developing training scenarios. Abstracted summaries of lessons learnt were also seen as a useful feature.

Including complex case studies

The inclusion of complex cases such as the refugee/migrant case study would be a big asset. It is precisely these 'out of the ordinary' or 'not in the textbook' cases which are tricky to capture that would provide very useful resources for 'lessons to be learned' and training.

Search

Many documents are publically available on google and there are many restricted sources, but one needs to know they are there to search for them. Added value could mean having a search function that could lead you to information that you didn't know existed.

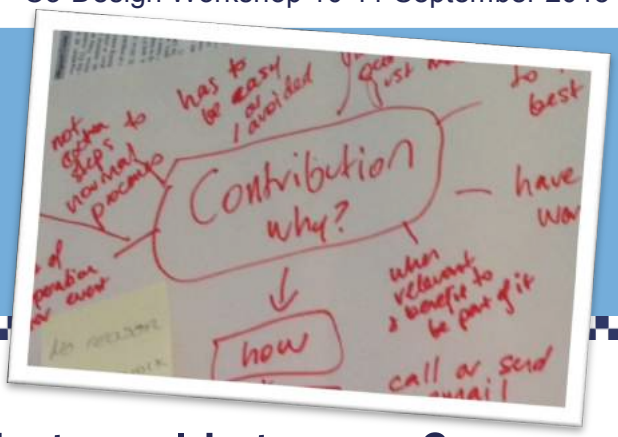
Moreover, big reports are often unwieldy, a way for the

Finding new partners

Participants saw value in having a system that could allow new partners to enter into collaborations if needed since, in the uncertainties of crisis, one might need partners one had not thought of before, let alone accommodated into information sharing agreements.

Sharing information

"No extra steps to daily business."



Why contribute information?

Practitioners identified many reasons why their organisation might contribute information to SecInCoRe.

This included developing common knowledge about how to manage a crisis, shared goals, preventing loss of organisational knowledge, having examples of best practice, and learning from others so you don't have to reinvent the wheel.

The point was made that to contribute one would need clarity about what the system offered. To, as one practitioner put it, 'be able to see the benefits'.

Stratification of access through the SecInCoRe concept could help with difficulties in establishing information sharing agreements, which often deal with each individual organisation rather than a collective.

What would stop you?

However, extra burdens on time or financial resources would prevent people from contributing to SecInCoRe. It had to be integrated with what organisations were already doing. Practitioners expressed that they

> *don't want to have to change [information] into another format. Don't have money to employ someone to do that.*

What would or wouldn't you share?

Practitioners felt their organisations would be willing to contribute general, non-sensitive information about an incident, including numbers and percentages; plans such as emergency evacuation plans; resources and services that the organisation could offer; and contacts (roles rather than names, as these can change).

There was concern about sharing sensitive and detailed information such as personal data and emergency plans as this would raise issues around confidentiality and data protection.

There were also concerns about sharing information that might convey that someone did something wrong, because:

> *If an organization knew it had to share incident debrief documents then you wouldn't get the same level of openness and honesty.*

This type of information was more likely to be conveyed in informal conversations.

What people would or would not share also depends on timing. Most often, information would not be made available immediately, but a case study or how a situation had been dealt with would be added once it had been filtered.

Some thoughts

SecInCoRe addresses these constraints and concerns through a range of design considerations.

Contributing does not have to be a conscious, special act of generating and 'donating' information. It entails different practices, such as ensuring that meta data and access policies for all pieces of information generated by an organisation were compatible with SecInCoRe so that they can be automatically 'picked up', with support for specifying access levels included.

Communicating across diversity

A matter of translation

Language arose as a key issue when sharing information within a pan-European context.

Practitioners discussed that while English is often seen as a common language, not all emergency responders use English and reports are often written in different languages.

However they also felt that translating information has its own challenges. It takes time and resources, and there were concerns about the accuracy and the liabilities of relying on online automated translation tools.

Moreover, even if all information was translated into one language this would not mean that terms would be used or understood in the same way.

Crossing Contexts

Translation also happens in other contexts. For example, information needs to be translated into how people at different levels in the incident management structure use it.

And how information is mobilised and understood would vary in relation to the phases in the emergency management cycle.

For example planners may have different information requirements to those involved in operations

Other challenges for communicating and working across agencies and international borders were also raised.

Emergel EU Taxonomy for Hazardous Substances
http://idi.fundacionctic.org/disaster-fp7-skosic/

Diversity

There is significant diversity in legal systems, which can impact how countries and organisations would interact within a common information space.

Organisations already have their own methods and networks, including 'secure networks' for sharing information.

Likewise, there is a wide diversity of emergency management models and practices that extend right down to an organisational level. As one practitioner said:

> *Every organisation in every part of every country does debrief documents differently.*

In addition, national and organisational approaches to roles and responsibilities differ.

For example, a job done by the fire brigade in Germany might be done by a different type of agency in another country.

Different understandings of terms and issues and even questions are impacted by cultural and organisational differences.

SecInCoRe Responses

Taxonomies and translation services are an integral part of SecInCoRe, including innovations developed elsewhere, such as the EMERGEL project.

But the challenges described here highlight that innovation cannot stand as technical innovation alone.

Usefulness of technical systems depends on social, cultural, organisational, policy and political innovation as well as training, communication and more useful and implementable standardisation.

SecInCoRe requires synchronised innovation on many levels. This is not something one research team can make happen and package into a product, but we can draw up a blueprint and make some of the components of the whole picture.

SecInCoRe after SecInCore: Sustainability

"Deliver something that will be sustainable into the future, that should be your focus."

A cafe style activity allowed the group to discuss different perspectives on four different models of 'sustainability' or business models for developing the SecInCoRe concept after the end of the project. These were a publically funded Pan-EU model, a commercial model, a not-for profit model and a 'vertical' model where the project is focused on one or two specific emergency related topics, such as flooding.

There were many common themes and the discussions significantly clarified the opportunities and challenges.

Publicly funded pan-EU

While there were concerns over the feasibility of a pan-EU system, advantages include opportunities for coordinated action, mutual learning, and The Mechanism. Such a model would enhance abilities to ensure continuity and was also felt to be an inclusive solution that didn't burden one individual country. It could embody and support European values and help address cross-border crises such as the refugee migration crisis.

However, a pan-EU publicly funded model was not without criticism. There is a need to avoid "typical EU issues" of bureaucracy/too many people involved and bickering, and there was a concern that the awareness and uptake of the system could be low. Furthermore, concerns were raised about differences between EU countries on issues such as data protection, organisational roles and responsibilities, language and culture, which could impede information sharing.

Commercial

Having the market underwrite the project raised interesting reactions. On the one hand, this was seen as an advantage that could provide incentives for SecInCoRe to be regularly updated and at the vanguard of innovation in order to establish itself or to become a market leader. On the other, concerns were raised whether market values would be counter to those of SecInCoRe and whether they would hinder rather than incentivise the development of the project (for example, in cases of market monopolies or of settling with doing just the minimum that is legally necessary).

Further concerns were raised around issues of ownership and control of the data, which were linked with issues of accountability, transparency and trust. Practically, the question of what happens if the commercial company dissolves or changes ownership was raised along with the need for EU accreditation in order to ensure trust in the system.

Non-Profit

Advantages here include the potential to be more agile and less bureaucratic. It might be closer to the field making it easier to collect data. A coalition of partners could provide balance through different perspectives and network building. However, key concerns were raised about the resilience and economic sustainability of a Non-Profit approach.

A lack of resources or funding, or the need to gain external funding could make for a fragile existence and complicate maintenance and upgrades. Concerns were raised around validity, security and trust especially with data coming from many sources, or organisations that had a particular agenda. A need for validation by official EU/UN mechanisms was raised. Other issues included questions about ownership and what would happen to the system/data if it becomes unsustainable and whether it would be possible to have restricted/sensitive data in such a context.

Vertical Implementation

The term 'vertical implementation' describes a sustainability approach that focuses on one or two specific emergency related issues, such as flooding or earthquakes. This could provide an easier way to find information or harmonise terminology across countries and attract specialists. However. If the selected topics are not at the top of the agenda of stakeholders in a specific period it will be difficult to keep up to date as attention will go to other topics. Command and control information for each service and country could be duplicated, although this could also be presented beside the vertical topic.

Similar trust issues such as having the hosting and control in public hands and the quality of information needing evaluation from a public authority were also present. It was also highlighted that such an approach would need to select a topic that was of interest for all EU countries and based on representative analysis of interest and need.

Last words

"… being a proof of concept surely we should be looking at the ideal, the ultimate - getting there [is] always going to be a journey- but what we're looking at is the end result and what it is going to achieve."

"For the project to succeed you need to get a prototype up and running and we need a driver or champion at the European level to guarantee the sustainability."

Word cloud of key issues in emergency response, gathered from introductory statements

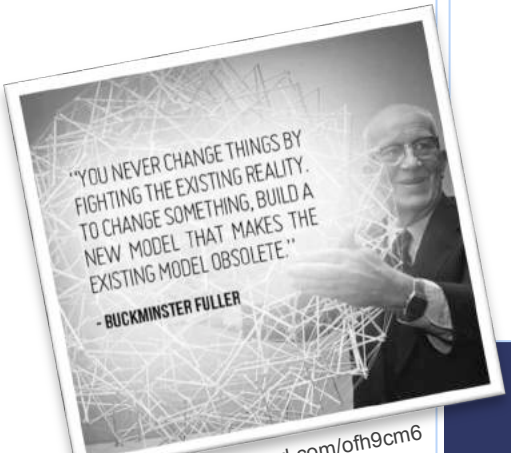
Where is SecInCoRe now?

SecInCoRe consists of two key elements: an inventory of past disaster events, data sets, 'lessons learnt', crisis management models and more and a Common Information Space concept that includes new technological and organisational opportunities to contribute and retrieve information.

This workshop did not focus on technology, but much has been done to implement and integrate software tools for SecInCoRe purposes.

The challenge now is to make the proof of concept concrete with a prototype and experimental implementations.

The Advisory Board experts, drawn from all over Europe and many organisations are not merely independent 'evaluators' of project results, but co-designers, central to this effort.



Let's do more work together

Feedback from Advisory Board members suggested that they would like to have more engagement with the project between workshops.

The project team would also like to develop greater and deeper engagements with Advisory Board members to further draw on their expertise. We are currently working out different options for doing this and welcome suggestions. Some ideas include:

- Follow up interviews or conversations on specific questions.
- Meetings at relevant events (such as FEU 2015 or http://www.esrdublin2015.eu)
- Co-design workshops where members can experiment with the IT components, discuss and enact organisational innovation.
- Reviews by members representing the same type of organisation in different countries.
- National workshops to make IT systems constantly available requesting feedback along the design and implementation path.

Thank you!

to all Advisory Board members for their