EPISECC Common Information Space: Defining data ownership in disaster management

Gerhard Zuba[1], Lina Jasmontaite[2], Uberto Delprato[3], Georg Neubauer & Alexander Preinerstorfer[4]

"*Disaster-affected people need information as much as water, food, medicine or shelter: accurate, timely information can save lives. The right information helps aid organizations to understand better the needs of affected communities and ways to meet those needs. Today's information technology presents new possibilities, but has not been fully exploited by humanitarian organizations. Lack of information can make people victims of disaster.*"

- World Disaster Report 2013, International Federation of Red Cross

1. Introduction

Advancements in the Information Communication Technology (ICT) have led to the growth of data that can facilitate the decision-making process in various sectors, including the public protection and disaster relief (PPDR). For the PPDR organisations, ICT tools can provide access to necessary information in a particular situation (e.g. a plan of the suburb in a case of fire). Timely availability of data can not only enhance situational awareness of first responders but also lead to better decisions when responding to crises. Yet many ICT tools used for Incident Command Systems for the PPDR primarily focus on needs of organisations on the operational level. This often results in a lack of interoperability of different information systems used by different PPDR organisations. This is of a great concern in transboundary emergency events, including natural or man-made disasters and environmental crises, where PPDR organisations need to cooperate and exchange information.

The number of information sharing platforms on the EU level has been growing. Usually these platforms serve only one purpose and focus on one particular issue. For example, the Critical Infrastructure Warning Information Network (CIWIN) allows to exchange critical infrastructure protection related information and the Common Emergency Communication and Information System (CECIS) contains info of Member States resources that could be used to respond to emergencies.[5] In addition to a limited purpose, these platforms are often based on voluntary participation and thus consequently have limited impact on enhancing coordination, cooperation and recognition of technical standards or specifications among organisations working in a specific field, such as PPDR.

[1] Frequentis AG, Vienna, Austria, gerhard.zuba@frequentis.com
[2] KU Leuven – Centre for IT and IP Law – iMinds, Leuven, Belgium, lina.jasmontaite@kuleuven.be
[3] IES Solutions, Roma, Italy, u.delprato@iessolutions.eu
[4] AIT, Vienna, Austria, Georg.Neubauer@ait.ac.at, Alexander.Preinerstorfer@ait.ac.at
[5] Critical Infrastructure Warning Information Network (CIWIN), Weblink: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm, accessed 03.06.2016.

To improve the current situation and address the needs of Public Protection and Disaster Relief organisations, the "Establish Pan-European information space to Enhance seCurity of Citizens" (EPISECC) project has been developing a Common Information Space (CIS).[6] This paper will provide an overview of various decisions taken when developing a common information space with respect to data sharing. The paper will aim at introducing the EPISECC Common Information Space (CIS). Consequently, the paper will explore the CIS user requirements and software architecture. The paper will also define a methodology to map data flows within the CIS and examine the basic functionality of the system. The underlying objective of this paper is to provide an operational overview of the EPISECC CIS.

2. Defining data flows and design process in the EPISECC: Why is it important?

In response to the changing nature of emergency management, the EPISECC consortium aims at developing an architecture which would facilitate information exchange between and among different types of first responders and PPDR stakeholders ranging from public authorities to private entities and NGOs contributing to relief actions in emergency events. Before the architecture has been defined, it has been important to engage in a discussion with a wider community about the EPISECC approach and decisions made throughout the system design phase. Explaining the step by step approach is valuable as it can help to improve acceptance of the CIS by the end users and allows identifying weak points of the proposed framework. In other words, sharing the EPISECC experience to a larger public, in particular to the end-user community, can enhance ethical acceptability, social value and scientific validity of the research and innovation efforts of the consortium members. Even more so, by provoking discussions it may allow to attain an acceptable ratio of potential benefits to risks or harm that may occur from the CIS to vulnerable populations.

At the same time, defining data flows within the CIS is important for the legal (sometimes referred to as regulatory) compliance purposes. Legal compliance is a quality aspect of ICT tools for PPDR organisations. It is reasonable to expect that only tools that were designed to conform to applicable regulatory measures, such as standards and laws, can be adopted by PPDR organisations.

Finally, data exchange and processing in PPDR include various types of data. Some of the data, such as personal data or data subjected to the intellectual property rights, is subject to a particular set legal requirements. Provided the highly fragmented nature of technology regulatory, ensuring regulatory compliance of ICT tools for PPDR prove to be very difficult. Numerous technical, operational and cultural standards exist in the field of the PPDR.[7] Therefore, defining and visualising data flows is valuable as it

[6] EPISECC is a Collaborative Project which will Establish a Pan-European Information Space to Enhance seCurity of Citizens, funded by the EU, grant agreement no. 607078.

[7] Examples of technical standards include: EMTEL TS 102 181 (Requirements for communication between authorities/organizations during emergencies), TS 102 182 (Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies) and TS 102 410 (Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress); CEN-CENELEC. CEN/TC391 (Societal and Citizen Security).

can help to identify applicable regulatory frameworks. Within the EPISECC project, legal compliance was focusing on access to information held by the public sector, intellectual property rights and protection of personal data. For the latter domain, defining data flows helps not only to carry out legal compliance assessments and define applicable data protection requirements, but also to conduct Data Protection Impact Assessment that evaluates the project against the needs and expectations, concerns of the relevant stakeholders.

To ensure the quality of information it is recommended to clarify the responsibilities of the engaged actors/organizations. The practice shows that better information quality is ensured if actors own the data they generate and create (e.g. the automotive industry). The attribution of data ownership also may help to answer questions about the control of the information flow, the cost of information, and the value of information.

Finally, defining data flows is of relevance to software developers as it can assist when developing the information governance strategy for a particular system as well and identify security flaws which can result from information exchange as well as anticipate functionality and security drawbacks. For example, it can ensure more precise understanding of data and complex system and define the chain of responsibility.

3. Information inventory and a data mapping exercise

To ensure compliance with the relevant regulatory frameworks and the expectations of organisations assumed to share their information, developers of CIS need to understand and determine what types of data are being processed and what types of data are stored in the system. For these purposes, the developers are suggested to pin down all information that could potentially be made available on the EPISECC CIS. Within the ESPISECC project this was done in Deliverable 6.1 "Proof of concept design", where a selected list of communications tools was analysed in greater detail. The overall objective of the information inventory is to determine:

- types of data producers (organizations that create, compile, aggregate, package, and provide information to be inserted into an information sharing system);
- what types of data are processed (e.g., weather forecast, personal information, structured, semi-structured, and unstructured information);
- purposes of information consumption (e.g., information about situational awareness, decision-making process);
- flows of information; and
- status or sensitivity of information (confidential, sensitive personal data).

While the data mapping exercise may allow to understand better what kind of tools can be connected to the CIS, it should be noted that it hardly ever leads to a complete and final document. Data mapping exercise continues through the lifecycle of the CIS and needs to be updated on a regular basis as different tools could be connected.

Certainly creating such an inventory contributes to the quality of the IT system. Yet "producing good software designs requires a considerable amount of practice, with a great deal of feedback on the quality of the designs with the resulting software products influencing the design of the next software system."[8] In other words, it requires human effort and is costly. Within the scope of the EPISECC project, the advisory board is regularly consulted about the CIS architecture.

4. Common Information Space: EPISECC Approach

Common Information Spaces have been deployed for complex governance in both the public and private sectors with complex governance structures to improve efficiency of activities carried out by an entity. Some attempts on the national level have been made with respect to developing information systems for PPDR, yet such attempts have not received much attention on the international level. To aid the current situation and enhance interoperability of different tools used for the PPDR, the EPISECC CIS will be based on the distributed processing implementation by peer to peer architecture. This means that there will be no dedicated servers and clients, instead all processing responsibilities will be allocated among all the machines that that are considered to be peers. To become a peer an entity needs to register.

This architecture ensures that there is no centralised data storage or information gateway which could become a single point of failure or a target of cyber-attacks, leaking sensitive or protected data. In fact, the information to be shared stays in the domain of the data owner and the implemented authorisation and data protection concept guarantees that every piece of information is only accessible by authorised participants. Apart from security related aspects, an additional advantage of the architecture is to ensure that messages are sent to the right address in shorter time. The possibility of selection of wrong email addresses and loss of time due to late decisions is considerably reduced.

5. Common Information Space and its objectives

The overarching aim of the EC funded project, titled "Establish Pan-European information space to Enhance seCurity of Citizens" (EPISECC), , is to enhance security of citizens by improving data management practices and information sharing capabilities between the various parties involved in responding a disaster situation. The main objective of the CIS that will be developed within the EPISECC project is to serve as a tool enabling interaction and optimising coordination of civil protection assistance in disasters of various scale, including disasters that prompt activation of the EU Civil Protection Mechanism.

a. Defining user requirements for the CIS

The first step in developing the architecture for the EPISECC CIS entailed a detailed analysis of the management practices of past disasters. For this purpose, a questionnaire was developed that served as an

[8] Leach, Ronald J. *Introduction to Software Engineering*, Second Edition, 2nd Edition. Chapman and Hall/CRC, 2016. Vital Source Bookshelf Online.

interface for the interviewees that represent the majority of the EU countries. In this context, more than 40 interviews with European crisis managers were performed. The interviews covered multiple types of disasters such as flooding (hydrological disasters), earthquakes (geological disasters) or complex events such as the management of the currently ongoing refugee flow. Taking all types of events into account, the predominant request was related to interoperability (34% of all requests). Out of these requirements, 30% were related to improved information exchange on tactical and or operational level, 26 % of the requests were dealing with information exchange on political/strategic level and finally 26% were related to technical interoperability requests.[9] The majority of examined disasters were predominantly events managed on a national level, the request on improved interoperability was therefore mainly related to the national level. In detail, those statements include predominantly requests on an improved operational picture, lack of shared information as well as requests on tools allowing improved information exchange including adequate interfaces for the crisis management tools of stakeholders. Other important requirements focus on the need of a common taxonomy as well as the problem of language barriers in case of border crossing crisis managements. Another set of requirement is focusing on request on technical solutions such as a general lack of adequate tools for communication and information exchange or missing resilience of communication tools. It was also pointed out, that main problems arise due to communication problems or political challenges. In addition, data protection requirements have to be integrated in any future solution.

Taken together, the requirements from stakeholders clearly demonstrate the need of an information space that allows interoperability of the very heterogeneous landscape of crisis management tools used by European stakeholders, including proprietary solutions. Following on the end-users' recommendations to integrate existing standards and taxonomies in the development of new platforms and to develop decentralized platforms instead of centralized approaches in order to avoid hosting and funding problems for the system to be installed in case of a disaster, the EPISECC CIS has been designed.

A CIS concept has multiple advantages compared to the current information exchange approaches that are based on direct connection of all systems of the stakeholders (see below Figure 1). Automatic sharing of information ensures use of correct addresses and saves time, assuring that measures can be taken faster in time critical situations. Moreover, the requested technical efforts are reduced in a long term, because it is only necessary to design one adaptor for each system connected to the CIS only once. There is not need to develop new interfaces each time a new system is included in a communication process.[10]

b. Sharing information

For efficient response to a disaster, access to necessary information, seamless communications between rescuers and stakeholders as well as the coordinated availability of resources are key factors. Additional challenges particularly in cross border events include language barriers, organizational and technical barriers hindering communication and information exchange. To improve the collaboration in these situations, new concepts like a common information space are necessary.

[9] EPISECC, Deliverable 3.4 "Pan-European inventory of disasters and business models for emergency management services", available at: https://www.episecc.eu.
[10] Could interoperability have prevented the metro bombing in Brussels?, Weblink: http://www.iessolutions.eu/en/interoperability-metro-bombing-brussels/, accessed 03.06.2016.

The Common Information Space represents an architecture for sharing information in an easy way between the IT systems of organisations engaged in disaster relief. Beyond pure data exchange, it also includes concepts how to bridge the different terminologies making the available data understandable, and dynamic authorisation for safe data access dependent on needs in a given situation. The basic idea is to share information automatically between tools of different organisations that do not have dedicated interfaces for daily cooperation. Instead of developing specific interfaces for every (potential) pair of partners, CIS provides standardised interfaces that need to be implemented only once per tool (CIS adaptor).

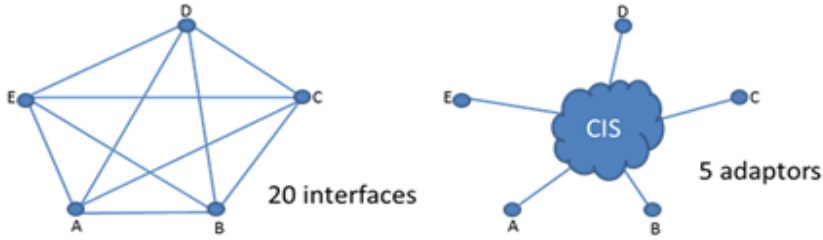

Fig. 1: connecting 5 communication tools without / with CIS

The shared information is transported within the CIS as standard messages, using both standard formats (e.g. CAP, EMSI), and uniform EPISECC taxonomy for key terms which are not predefined by the used standard definition and namespace. While creating/interpreting the standard messages sent/received via CIS, the CIS adaptor has to transform proprietary interface formats of the connected tool to the CIS standard syntax and semantic. That means the adaptor has firstly to transform the parameters of the tool used by the sending organisation to the elements of the used standard and backwards at the receiver side (*syntactical interoperability*).

As a second step, it has to map the terms and keywords used by the tool (organisation owning a tool connected to the CIS) with standard terms used in CIS, in other words *semantic interoperability*. This comprises both, mapping of proprietary terms to key values defined by the standard, and mapping of proprietary terms to values representing the standardised EPISECC taxonomy (free text will not be translated by semantic mapping). To overcome possible limitations in the coverage of terms in the taxonomy, the project has introduced the concept of "broad match", according to which, each term will be available on the receiving end either as an "exact match" or flagged as having the closest meaning (taxonomy). The more the taxonomy will be used and enriched, the more accurate matches will be offered to the users. The transmitted information will always contain both, the originally sent message providing accuracy and the semantic annotations providing an easier understanding for the receiver.

All business logic and the ownership of information stay with the tools participating in information sharing. The common information space itself does not create, own or process the data. It is not a central data repository, but just an information broker that distributes information that is released for sharing with defined partners.

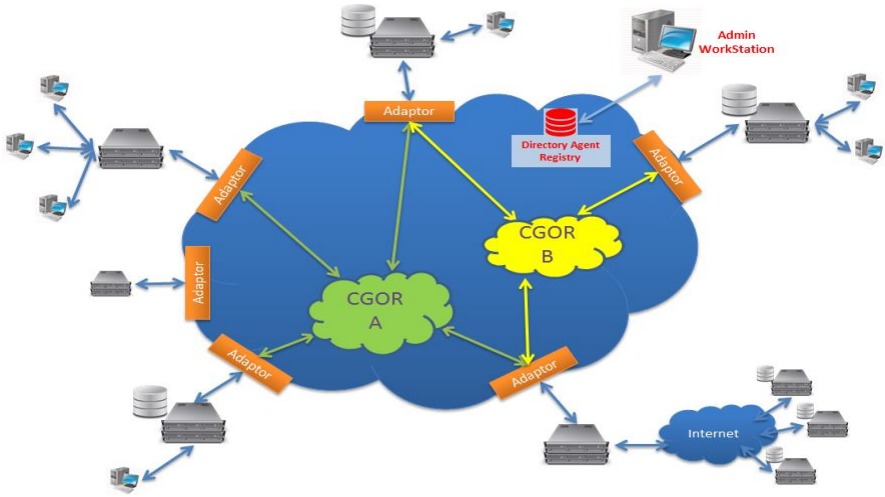

Fig. 2: Sharing information via CIS

The standard-based adapter concept ensures information exchange without the need of knowing the interfaces and terminologies of other partners. That allows ad-hoc integration of new tools or services without modifying existing adaptors.

Beyond the technical capability for automated data sharing, trust between the partners and confidence in data security and integrity is key for the acceptance and willingness of organisations to share their information. A context aware and configurable security concept is integrated in the CIS architecture. The trust policy requires the registration and certification of the CIS participants. Communication Groups and Online Rooms (CGOR) can be established dynamically according to current communication needs, and only the trusted and accepted participants are able to read or publish the information circulated in a CGOR. Data wrapping and encryption related to the CGOR prohibit unauthorised use of the shared information and minimises security risks. While the CIS concept provides appropriate tools for configuring safe communication groups, the responsibility for the classification of information and the lawful handling of sensitive date remains with the participating organisations and their tools.

6. Conclusion

It is important to note that the EPISECC project does not intend to replace existing and successful operational procedures of first responders. It rather aims at creating an information platform that would assist PPDR organisations with additional information and with the capability for cooperation. Simple but effective collaboration procedures shall be added in order to achieve acceptance within the stakeholder community. The operational capacity of CIS will be first tested in the proof of concept of the EPISECC scenario. This scenario will demonstrate the extent to which the CIS architecture is of relevance, actuality

and completeness of shared data, when it comes to information sharing between different types of first responders acting jointly in transboundary emergency events and crises.
A prototype implemented for the proof of concept exercise will comprise the CIS distribution mechanism including the data protection components and adapters for tools that the project partners bring in, as well as samples of taxonomy from the participating end-user organisations.

This paper was made possible thanks to the funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under the EPISECC project (Establish Pan-European information space to Enhance seCurity of Citizens), grant no. 607078.

References

Could interoperability have prevented the metro bombing in Brussels?, Weblink: http://www.iessolutions.eu/en/interoperability-metro-bombing-brussels/, accessed 03.06.2016

Critical Infrastructure Warning Information Network (CIWIN), Weblink: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm, accessed 03.06.2016

EPISECC, Deliverable 3.4 "Pan-European inventory of disasters and business models for emergency management services", available at: https://www.episecc.eu

Leach, Ronald J. *Introduction to Software Engineering*, Second Edition, 2nd Edition. Chapman and Hall/CRC, 2016. VitalSource Bookshelf Online

World Disaster Report 2013, International Federation of Red Cross, Weblink: http://worlddisastersreport.org/en/chapter-3/index.html, accessed 03.06.2016