J Ambient Intell Human Comput (2015) 6:783–795
DOI 10.1007/s12652-015-0283-x

ORIGINAL RESEARCH

Advanced services for critical infrastructures protection

Rafał Kozik[1] · Michał Choraś[1] · Adam Flizikowski[1] · Marianthi Theocharidou[2] · Vittorio Rosato[3] · Erich Rome[4]

Received: 28 February 2015 / Accepted: 29 May 2015 / Published online: 6 June 2015

Abstract In this paper an overview of the first results of FP7 CIPRNet project is presented. Particularly, we demonstrate CIPRNet services for critical infrastructure protection (CIP) stakeholders. The role of the proposed services is to support decisions in the CIP domain. Moreover, those services are expected to serve as the underpinnings for the European Infrastructures Simulation and Analysis Centre (EISAC) which, similarly to the US NISAC, should provide operational services on CIP, for the benefits of CI operators, stakeholders and the Public Authorities committed to CIP.

Keywords Critical infrastructure protection · CIPRNet project · Decision support · Services · Modelling and simulation

✉ Michał Choraś
chorasm@utp.edu.pl

Rafał Kozik
rkozik@utp.edu.pl

Marianthi Theocharidou
marianthi.theocharidou@jrc.ec.europa.eu

Vittorio Rosato
vittorio.rosato@enea.it

Erich Rome
erich.rome@iais.fraunhofer.de

[1] University of Science and Technology, UTP, Bydgoszcz, Poland

[2] European Commission, Joint Research Center, Institute for the Protection and the Security of the Citizen, Ispra, Italy

[3] ENEA Casaccia Research Centre, Rome, Italy

[4] Fraunhofer IAIS, Sankt Augustin, Germany

1 Introduction

Critical infrastructures (CI) protection (CIP) is a complex and delicate task. From one hand, decisions taken for CIP purposes may impact human lives and material goods, threatened by both natural phenomena as well as the consequences of human errors. From the other hand, such decisions must be taken in real-time—particularly during the CI-related crisis (European Council 2008). Most often such decisions are taken by analysing a large amount of heterogeneous data.

In CIP domain, this challenge can be presented in three dimensions, called 3 V model of Big Data problem (Gartner Inc. 2011). These three dimensions include:

- Volume of data, that must be processed to build an actual picture of operation needed to take the appropriate decision in given time;
- Velocity of the constantly changing data provided to the decision maker from various sources, and;
- Variety of data that come from heterogeneous sources, challenging the reasoning and information correlation.

In this paper, the services for CIP community and decision makers are presented to support decision-making process in CIP, both in the preparedness ("cold") phase, as well as in the crisis ("hot") phase.

The goal of such services development is to increase the situational awareness of decision makers by extraction of the most necessary information from the large amount of heterogeneous data coming from different sources (such as real-time sensorial data).

Specification and development of the services proposed in this paper are the objectives of the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project—ongoing security research, co-funded by the

European Commission's 7th Research Framework Program (FP7) (CIPRNet 2015).

In the first phase of the project, the end-users community was asked to express and share their needs and expectations related to increase effectiveness of modelling, simulation and CIP-related analysis environment and decision making process.

In this paper, the analysis of their requirements is provided as well as the description of the demanded services that will later be designed in the CIPRNet project.

The rest of this paper is structured as follows:

- Section 2 presents the CIPRNet project,
- Section 3 focuses on end-users views and needs that contributed to the specification of CIPRNet services,
- Sections 4 and 5 present CIPRNet DSS services and CIPRNet VCCC services, respectively,
- Section 6 discusses non-technical aspects of CIPRNet services,
- Section 7 concludes the paper.

2 CIPRNet project

The Critical Infrastructure Preparedness and Resilience Research Network or CIPRNet (CIPRNet 2015) establishes a Network of Excellence in CIP. CIPRNet performs research and development addressing a wide range of stakeholders including (multi)national emergency management, critical infrastructure operators, policy makers, and public authorities. By integrating resources of the CIPRNet partners acquired in more than 60 EU co-funded research projects, CIPRNet is going to create new advanced capabilities for its stakeholders. A key technology for the new capabilities will be modelling, simulation and analysis for CIP. In order to achieve its mission, CIPRNet's Joint Programme of Activities has four major threads:

- Providing new capabilities to end users for better preparedness for CI-related emergencies:
  - An advanced decision support system enabling the prediction of risk on CI based on consequence analysis,
  - 'What if'—analysis for exploring different courses of action,
  - Support of secure design of next generation infrastructures,
  - 'Ask the expert' service for demonstrating timely, actionable, risk-informed CIP analyses and strategies for authorities,
- Building required capacities by educating and training experts and researchers (reaching a critical mass),
- Providing knowledge and technology to end users for improving their understanding of the role of CI in crises and emergencies: simulators, middleware, models,
- Providing long-lasting end-user support by establishing a Virtual Centre of Competence and Expertise in CIP (VCCC).

The project started on March 2013 and will be completed on February 2017.[1]

3 CIP end-user views collection

One of the first tasks performed by the CIPRNet consortium was to identify the needs arising from CIP communities, by a direct interaction with end-users and domains' stakeholders. The identified stakeholders relevant to the project represented the public, private, research and academia domains. The methods for gathering user views in the CIPRNet project were face-to-face meetings, remote user interviews and the CIPRNet questionnaire, filled in by the project end-users and domain experts. Outcomes of the collected questionnaires were a starting point in requirements specification process towards specification of solutions described in this paper.

The questionnaire was designed in order to provide a broad view on current end-user problems, limitations and expectations, including big data issues. Most of the questions were presented in an open or semi-open format. Therefore, respondents were neither limited in expression of their opinions, nor biased by pre-defined options to choose.

Generally, the questionnaire has been divided into four blocks of questions, namely:

- General information about the respondents, particularly their organisations, range of activities, matter in which he/she acts,
- Questions related to accessing the information, particularly concerning availability of information about CI coming from private and public sectors and used during CI-related crisis,
- Questions about using decision support systems during respondent duties, providing information about decision support mechanisms and tools, their limitations, data exchange, standards, etc.,
- Questions about simulation and modelling for CI crisis management purposes.

Respondents, who filled in the questionnaire, represent various organisations—from local and regional CI-related organisations to Pan-European agencies, and from

[1] More information about the CIPRNet project can be found at project website: www.ciprnet.eu.

academic and applied researchers to CI-operators. However, the majority of respondents are representatives of organisations that operate within nationwide range, and usually as public emergency/crisis management centre.

3.1 Accessing the information

The respondents assessed availability of various information related to CI from various sectors and sources and gave them ratings. According to respondents' ratings, generally there are no significant differences between levels of availability of information, when comparing public and private sectors. The average ratings for public vs. private CI information availability (e.g. geo-localisation data, operational data and sensitive data about these infrastructures) are at the similar level. Considering information about CI dependences, it is noticeable that such information during normal operation is significantly easier accessible than during non-normal state of operation.

The questionnaire analysis shows that the hardest categories of information to be accessed include:

- Operational data of private sector CI,
- Information about CI across the national/regional borders,
- Information about CI across public–private sector borders,
- Information about CI dependencies during non-normal operation.

In addition, respondents indicated that reliable data of CI financial aspects and CI failure status are also not easy to obtain from CI management entities.

According to end-users,

- Climatic and weather information for specific (emergency) area, and
- Geo-location information about public/private sector CI,

are described as the relatively easiest to obtain.

Concluding, most of the categories (excluding e.g. mentioned climatic/weather data) of information considered in the questionnaire were assessed as relatively hard to obtain. This observation indicates a serious problem related to information accessibility, and what is worth noticing, challenges related to acquisition of necessary information exist regardless of the CI functioning sector (i.e., private versus public).

3.2 Decision support systems

About 40 % of respondents reported that they do not use any ICT-based support for their decisions. The majority of remaining 60 % of respondents stated that they (or their organisations) use internally developed tools for specific purposes of their organisation, or alternatively, that they use various loosely coupled data sources (such as GIS resources, the weather data, etc.) to support decisions. Specific DSS tools used by interviewees have been listed, such as C3 M, IPCR or WebEOC. These systems are exploited for the crisis response planning, reporting, procedure and policy creating, resource allocation and tracking.

When asked about the analytical capabilities, as well as about usefulness and effectiveness of these systems during crisis-related decision-making, respondents presented different views. About half of them admitted that the used (DSS) systems do not meet their needs and that these systems are not tailored to the specific needs of their operation. As respondents emphasised, the main weakness of these systems is the need for advanced customisation (costly in terms of time, efforts, financing, etc.).

Other drawbacks include:

- Lack of interconnectivity with the other systems (e.g. used by entities cooperating with stakeholder's organisation during CI-related crisis),
- Lack of possibility to integrate the data from other entities/systems, hampering the cooperation between various organisations,
- Limited capabilities of spatial visualisation of threats, and
- Lack of capabilities to support comparison of the current situation to earlier forecasts.

Cross-border decision-making is another open gap of the used systems, impacting end-user operation.

The CIPRNet interviewees listed also various kinds of information sources that are used for building situational awareness in the emergency response efforts. These include mainly external sources such as cooperating entities and agencies involved in emergency response, which provide hydrological data, weather forecasts and information about CI (including geo-location). Other sources of information are the direct reports from the field/emergency area. Usually, such information is not publicly available. However, end-users can access that information in real-time or near real-time.

3.3 "What-if", consequence and CI dependencies analyses

Respondents stated that the primary need for simulation models relates to consequences of CI object failure, employing e.g. cascade models of infrastructure failures. End-users indicated different scales of such consequences, varying from impact on another single system, up to consequences for national security, societal impact, national economy, etc.

Moreover, respondents noticed lack of models supporting estimation of CI restoration time, identification of critical nodes (supporting CI objects prioritisation) and simulation models relevant to a given, specific sector (e.g. applicable for health care services during CI failure).

Asked for what should be improved in relation to decision-support for emergency management, respondents identified four main areas of interests:

1. Simulation and modelling, in particular development of threat modelling and forecasting tools, e.g. for simulation of the consequences of possible decisions.
2. Estimation of crisis impact, both on low level (e.g. impact of CI object failure on e.g. hospital functioning), as well on higher level—for example estimation of CI failure costs including national economy losses.
3. Emergency communication, namely: (a) information/data sharing, (b) timeliness of received information, (c) exchange of information among cooperating agencies and organisations in real-time, (d) compatibility of data formats and (e) mechanisms to support informing about hazards, etc.
4. Cooperation and training between solution providers and emergency management teams. According to the respondents, closer public–private cooperation also could improve the current situation in decision-making. The respondents also indicated problems related to the current assessment of CI dependencies. The most significant examples include:
    - Limited capabilities of simulations, particularly in terms of simulating interrelations between various CI and analysing the threats based on such relationships.
    - Organisations' and CI operators' isolation. In other words, organisations often do not effectively take into account consequences of their infrastructure failures, exceeding beyond their organisations and impacting other sectors, companies, etc.
    - Lack of systematic planning of CI protection and restoration after a crisis, as well as lack of procedures supporting such protection.
    - Problems with identification of contact points that in a case of crisis should be immediately available for responsible entities.
    - International standardisation in the CIP area.
    - Information accessibility.
    - Data validation and reliability.

3.4 Key findings related to user requirements

The end-users needs, expectations and requirements (presented in previous subsection) can be categorised into the following aspects related to the decision support process, simulation and modelling and access to the real-time data and critical information.

The key findings that have been identified after the analysis of the mentioned aspects are as follows:

- The end-users expect more advanced, customised and tailored (to their needs) decision support solutions, which will allow for flexible spatial threats visualisation, easy integration with new data sources or other systems, and information sharing between different entities engaged into a crisis management process.
- The end-users lack accurate models and simulation tools allowing for consequences, impact and risk analysis of CI failures and cascading effects. The forecasting capabilities are emphasised as one of the most desired.
- The end-users articulated the need of access to information related to CI from various sectors. They emphasised difficulties in gaining data related to operational state of private sectors CI and CI-related information across public–public and national-regional borders.

The requirements identified in the survey were the basis for the development activities in CIPRNet WP7 ("Decision Support System with consequence analysis"). More precisely, they were used as guidelines for further work, such as the final system specification and particular the CIPRNet DSS components development. Moreover, the survey results also influenced the work in WP6, complementing the description of the requirements for a cross-sector simulation environment and adding the end-user perspective into the development of application scenarios and the realisation of a demonstrator.

However, it should be mentioned that CIPRNet general requirements were focused on the decision support front-end, rather than on the back-end (the back-end consists of the models and simulations that provide the input information for the CIPRNet DSS).

4 CIPRNet DSS services specification

In order to cover the key findings (described in the previous section) coming from the end-user perspective analysis, the following DSS services have been specified: consequences analysis, threat forecasting (TF), threat visualisation, data accessing and gathering. It is expected that the functionalities and the number of services provided by DSS will evolve over the time. The proposed DSS will have two distinctive operational modes, namely "Hot Phase" and "Cold Phase" decision support (Fig. 1).

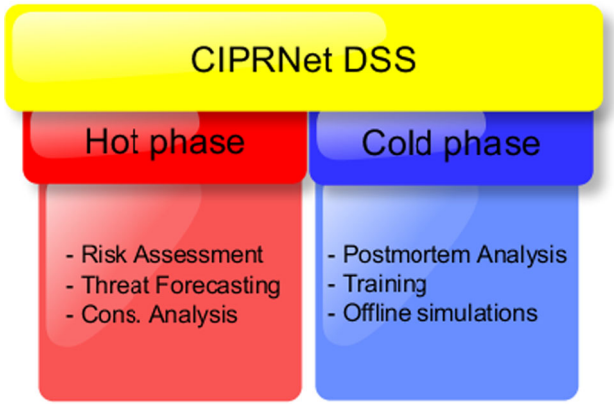

Fig. 1 Operational modes of the CIPRNet DSS

The "Cold Phase" is computationally intensive and therefore it is dedicated to post-mortem analysis and critical infrastructures operators training purposes. Among others it will heavily rely on historical data, modelling and simulation analysis (MS&A). The "Hot Phase" includes continuous and real-time risk assessment, threat forecasting and consequences analysis, which is being conducted using real-time data during the real crisis. These aspects are explained in next sections.

4.1 Data accessing and gathering (DAG)

This service provides the DSS with data needed to run the CIPRNet DSS workflow and with all information useful to mitigate and manage a crisis/emergency due to CI failures. In particular, the DSS-DAG service feeds data to the DSS-TF service that has the aim to forecast the possible natural phenomena that, potentially, can produce physical damage to CI components in a given area.

The DSS-DAG service will allow gathering and storing DSS relevant data to the CIPRNet DB (CIPRNet database). The data stored within the CIPRNet DB belongs, in general, to different pre-defined layers:

- Territorial layer,
- Socio-economical layer,
- Technological infrastructure layer,
- Historical events layer.

Each layer can be divided into sub layers. For example, the historical events layer can be further divided into geological (e.g. earthquakes), geomorphological (e.g. landslides), hydro-meteorological (e.g. floods) historical events layer.

Data sources can be governmental repositories (e.g. the national GIS repositories as the Italian SINANET site, the Italian National Institute of Statistics—ISTAT), CI operators, data coming from simulation models such as the weather forecast data that needs to be logged in order to allow different kinds of offline analysis (e.g. statistical analysis).

In general, data stored within the CIPRNet DB will require a different frequency of update operations. For example, the number of people living in a specific area needs to be updated once a year, while the historical events layer data (e.g. the earthquakes events in a specific area) needs to be updated with a frequency of minutes or hours. The update procedure is performed by using different modalities depending on data availability and update frequency requirements. In some cases, the data updating operations will depend on authorised data scraping automated procedures. The CIPRNet DB stores available historical data (e.g. rain precipitation data) and allows the development and the maintenance of historical series of data. The CIPRNet DSS can also use external repositories (e.g. via GIS WMS protocols).

4.2 Threat forecasting (TF)

This service provides the DSS with the capability to forecast natural events that have the potential to harm CI components (e.g. heavy rain, flooding, landslide, drought, heat wave, etc.).

The capability to predict a possible natural phenomenon that, potentially, can produce physical damage to the CI components in a given area is one of the key features of the DSS. The DSS-TF is composed of different modules, each dedicated to a specific source of perturbation to be monitored. In particular, the DSS-TF through the data accessing and gathering services will acquire different kinds of data: weather forecast data, now-casting data, earth observation data. Each module will use this data to run specific models to forecast specific threats on a specific area. For instance, the Flooding module will acquire data that can be used to forecast flooding events in a given area (e.g. abundant and prolonged precipitation, pluviometric monitoring sensor networks) followed by the run of hydrologic and/or hydraulic models to predict the flooding dynamics. The plug-and-play and easy to extend architecture of the DSS will allow connecting the CIPRNET DSS modules, which will be implemented to provide specific threat forecasting capabilities for specific areas. Indeed, the DSS-TF service can be configured in order to rely on already available data and models. For example, an instance of the DSS-TF Flooding module for the city of Rome can be configured to include the available data, which is related to the monitoring sensor network owned by the Autorità di bacino del Fiume Tevere (Tiber Basin Authority). The main modules to be included in the DSS-TF service are e.g.: flooding, lightening, landslide, strong wind, heavy snow, heavy rain, cold wave, heat wave, etc.

Table 1 Threat strength matrix

Threat level	1	2	3	4	5
Earthquake (ground acceleration)	0	0	0	0	0
Strong wind	0	0	**1**	0	0
Lightening	0	0	0	0	0
Heavy snowfall	0	0	0	0	0
Ice	0	0	0	0	0
Landslide	0	0	0	0	0
Flash flood	0	0	0	0	0
Flooding	0	0	0	**1**	0
Mud flows	0	0	0	0	0
Debris avalanches	0	0	0	0	0
Heavy rain	0	0	0	0	0
Strom surge	0	0	0	0	0
…	0	0	0	0	0

For each CI component, the DSS-TF service will produce a threat strength matrix that represents the probability that the given threats will materialise in a given area with a specific strength. Table 1 is an example of a threat strength matrix for a given CI component. The rows of the matrix represent the considered threats and the columns the threat strength. The matrix entries indicate the probabilities that the CI component will be affected by a threat of a strength as indicated in the column value. Considering the example presented in Table 1, the DSS-TF service indicates that the specific CI component will be impacted by a flooding event of strength 4 and by strong wind of strength 3.

The threat prediction matrix will be "cross-checked" with the vulnerability matrix (which is a characteristic matrix of each CI element) representing the specific vulnerability threshold of the each CI element with respect to each "predictable" event (i.e. each event which could be predicted together with its strength, as in the threat strength matrix). In this respect, the vulnerability matrix has the same entries (in the rows and in the columns) of the threat matrix: differently from the former, it contains the threshold for the resistance of the CI elements to the different perturbation sources. For example, let's suppose that the vulnerability matrix for the transformer TR1 indicates that the element is vulnerable to flooding of strength 4. If the threat strength predicted for the area where TR1 stands is as that reported in Table 1, this will indicate that the TR1 element will be likely to be damaged by the flooding and in the subsequent flow of computation, the DSS will predict the TR1 element in fault (when the predicted threat will manifest) and further evaluate Impacts on services and Consequences on different Sectors.

Figure 2 shows the main components of the DSS architecture that realise the DSS-TF.

The data accessing service, a component of the data accessing and gathering service, acquires data from external sources. This data is acquired and stored within the CIPRNet DB and is being employed by the different threat prediction modules to forecast the threats and to build, for each CI component, the threat strength matrix. The DSS-TF realises a specific workflow for the earthquake case. Indeed, the earthquake events are monitored by the DSS through the acquisition of raw data from seismic sensor networks and/or the reported measured shake maps. This data (e.g. earthquake epicentre and magnitude, ground tangential acceleration and the macro-seismic intensity) is being employed by the earthquake processing data module

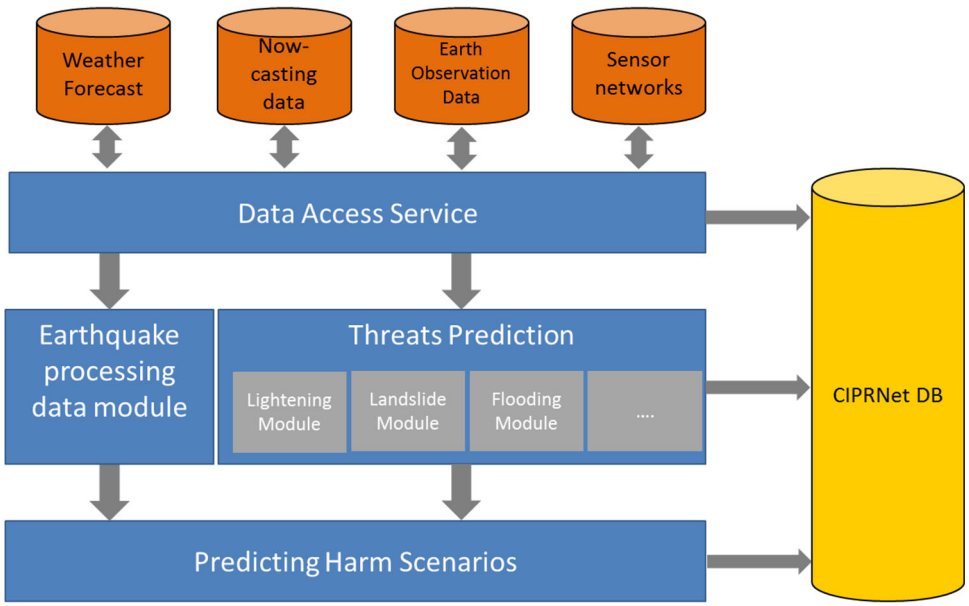

Fig. 2 DSS threat forecasting architecture

to compute detailed shake-maps. Those will be used to assess the impact of an earthquake event.

The input to the DSS-TF service includes different sources, namely: meteorological data (including weather forecast data and now-casting data), sensor networks data, earth observation data, and historical data (including landslide data and lightening data).

4.3 Threat visualisation (TV)

Visualisation is one of the key functionalities of the DSS. This section introduces the key functionalities that a visualisation service should provide in order to fulfil the CIPRNet end-user requirements.

The role of the service is to use different means to visualise a wide variety of aspects related to the decision support process, such as:

- Consequences analysis (e.g. consequence of impact on CI or its components).
- Threat forecasting (e.g. prediction of natural disasters like flood which may impose threats to CI).
- Risk assessment (e.g. with respect to the CIPRNet project consequences criteria).
- Analysis of emergency situations/scenarios, and assessment of how such scenarios may evolve, including the visualisation of possible courses of actions.
- Assessment of how big is the geographical area that has been impacted by the natural hazard.
- Prediction of possible effects of the natural hazards (e.g. using cross-referenced layers of geographical regions combining spatial information about the CI and natural hazards).
- Identification of the factors that may have influence on further development of the crisis scenario (changing weather conditions, probable threats coming from objects or CI located in impacted area).

The key element in the architecture of the DSS for emergency management is the GIS. Therefore, the DSS-TV should incorporate this visualisation technique in order to communicate wide variety of decision support aspects. Particularly, such visualisation must provide:

- An efficient and flexible way to access the threat visualisation data (e.g. web-based through web-browser or desktop GIS clients). An example of web-browser GUI is shown in Fig. 3.
- The ability to handle multiple simultaneous requests for visualisation (e.g. centralised web-based repository that is able to handle multiple read/write concurrent connections).
- The ability to share the provided visualisations among private and public stakeholders, emergency managers and common citizens involved in the disaster response.

Figure 3 shows the Database layers widget on the left. The represented GIS map visualizes all historical earthquakes in the considered area with an appropriate colour/shape code allowing to represent both magnitude and depth of the quake.

Figure 4 illustrates the use of GIS visualization in CIP context. Figure 4 (left) shows a flooded area while the right part of the Fig. 4 shows the extent and the position of roads which have been impacted by the event (as resulting from DSS Impact analysis). The colour code used for roads allows to indicate the minor (green) and the higher (red) impacts on them.

In Fig. 5, the map of the flooded area has been additionally enriched with the contextualization of the elements of electrical infrastructure (such as electrical transformers, high-voltage power lines, etc.) present in the flooded area. The estimate of the physical damages inflicted to the CI elements allows the DSS to design a "crisis scenario" whose simulation allows to predict the Impacts caused by the hazard to the Service level of the wounded CI and to the others which are functionally connected to it.

The general deployment diagram is shown in the Fig. 6. The visualisation service will expose a typical web-based client–server architecture. The client will communicate with the web server over the HTTP(S) protocol. The visualisation will strongly depend on WebGIS (responsible for spatial data manipulation) module and CIPRNet DB.

4.4 Consequence analysis and "what-if" analysis

Consequence analysis is a service included in CIPRNet DSS, that offers the added value to the decision making process. This service enables decision-makers and operators to perceive the possible extent of the impacts (produced by the physical damages) on the service granted by the interested CI. Consequences are measured in terms of the effects induced by reduction (or loss) of services on

- population
- environment
- industrial sectors
- management of primary services

These are the most relevant sectors which are prone to be hit by infrastructures services losses. Electrical outages could produce serious threat to old-aged population, service reduction to hospitals, unavailability of schools, reduction of public transportation functionality etc. Consequence analysis thus attempts to estimate those consequences, the extents of which are measured according to specific metrics. They will thus allow decision makers to have a complete "perception" of the crisis whose extent

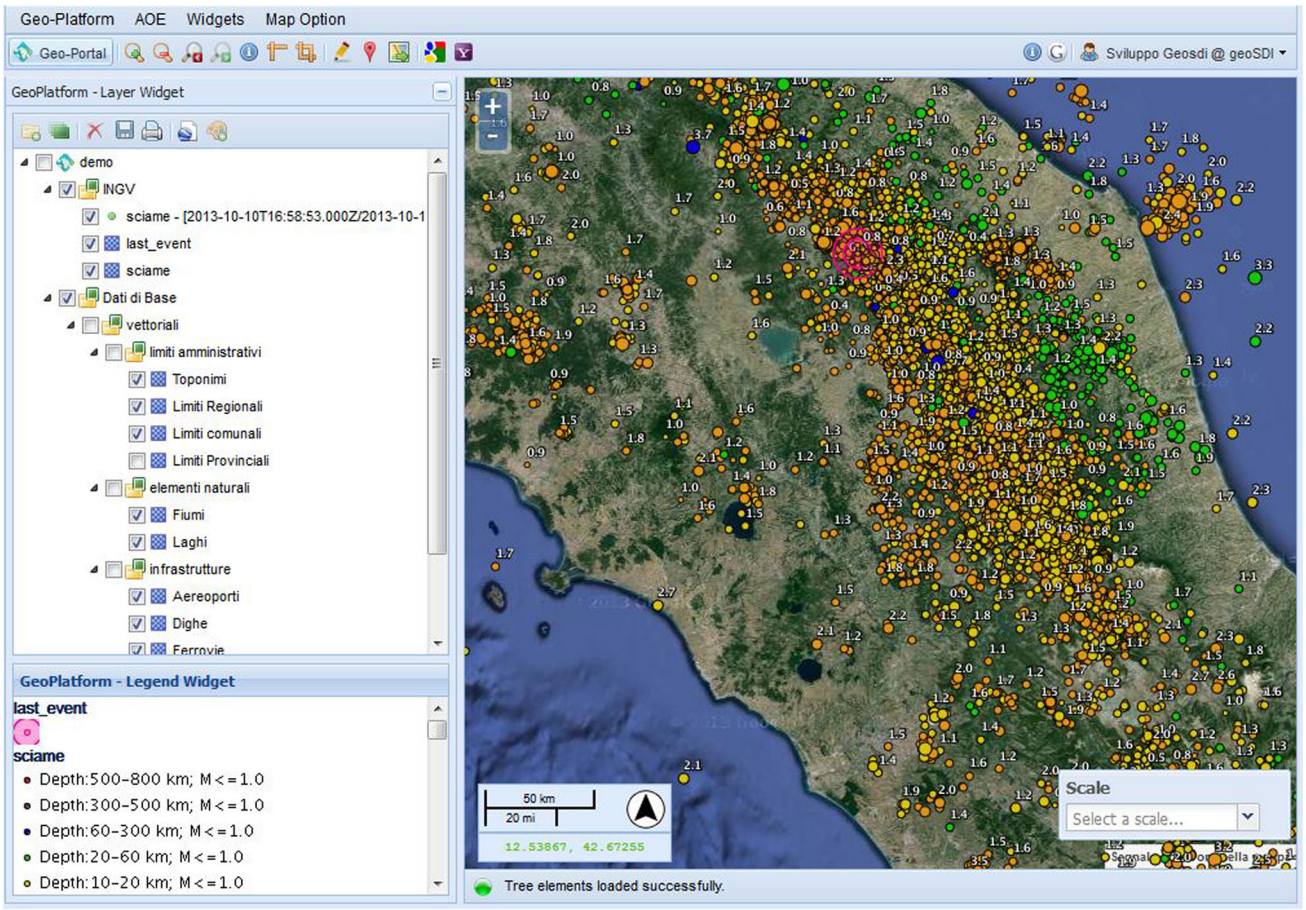

Fig. 3 Example of web-based DSS GUI

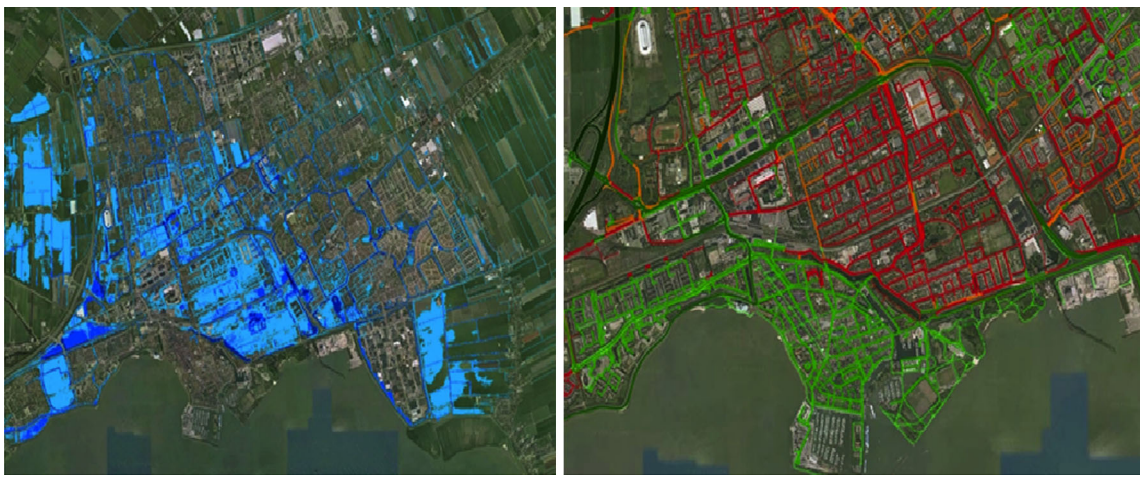

Fig. 4 Examples of different layers. *Left-hand side image* indicates the flooded area (*blue region*). The *right-hand side image* shows the transportation infrastructure that has been impacted by flood (*red colour*) (colour figure online)

can be evaluated in terms of "lives in danger", economical losses (for the industrial sectors), level of functioning of primary services (schools, hospitals, public transportations etc.).

"What-if analysis" (WIA) is one of the CIPRNet services that main goal is to provide the end-user with the simulation capabilities, which allow CI-related aspects to be investigated. Among others, the "What-if" will provide

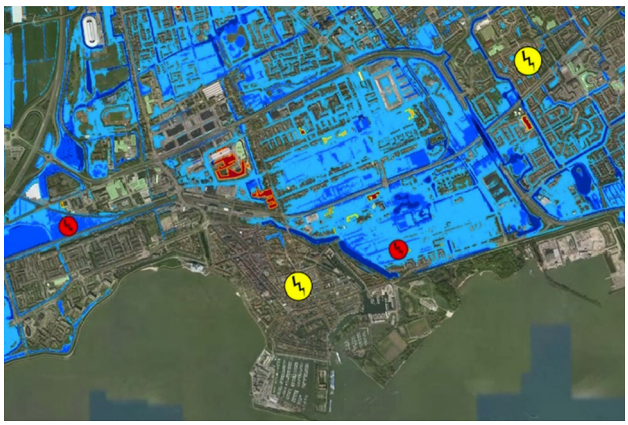

Fig. 5 Example of a layer showing electrical infrastructure impacted by flooding

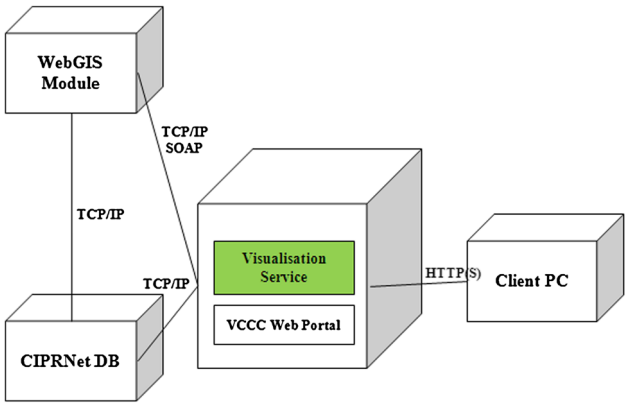

Fig. 6 Visualisation service—deployment diagram

the end-user with tools, which will allow them to analyse different crisis scenarios that may affect critical infrastructures. The analysis will allow the end-user to investigate different courses of actions and to evaluate their consequences. The core functionalities of this service will be enabled with tools and frameworks for federated simulation (Rome et al. 2009). The underpinnings for this have been established by DIESIS (Usov et al. 2010; Masucci et al. 2009) project, which CIPRNet is successor of.

The new capability of "what if" analysis will consist of a complex backend system setup including a distributed federated simulation, database components, and additional modules like consequence analysis. A full deployment of the new capability as stand-alone web application seems currently not advisable, since the usage of the capability requires end-user training and modelling support. Therefore, the VCCC portal shall provide an interactive "what if" analysis mock-up for demonstrating the functional principle of CIPRNet's "what if" analysis capability. The interface of the mock-up needs to be simple and intuitive, so that no special training for its use is required.

The expected users of this service include the management level of public authorities and CI stakeholders. The effects of using this service can be twofold:

- Dissemination of knowledge and added-value of CIPRNet's WIA capability,
- Attracting end-users to CIPRNet's training events on the real WIA system.

5 VCCC (Virtual centre of competence and expertise in CIP) services specification

Virtual centre of competence and expertise in CIP is a comprehensive repository of the tools, the technologies and the data developed and collected in CIPRNet (and in the previous CIP projects). During the course of CIPRNet, the consortium will elaborate, describe and defined (also at the Business level) the transformation of the VCCC into a new EU-wide asset, the European Infrastructures Simulation and Analysis Centre (EISAC) which, similarly to the US NISAC, should provide (at national scales, through national EISAC implementations, and on a pan-European scale, through the interaction of the national chapters) operational services on CIP, for the benefits of CI operators and stakeholders and the Public Authorities committed to CIP and to granting primary services continuity.

5.1 "Ask the expert" service

5.1.1 Description

The "Ask the Expert" service will be a component of the CIPRNet VCCC portal and will be accessible via the VCCC. End-users will submit questions and requests for information from the CIP domains. Questions can be related (however, not limited) to technical CIP-related issues, CI management, crisis management for CI, CI-related documentation, e.g. national and EU regulations, policies, public reports and statistical data and practical aspects of CI functioning.

The expected users of this service include public authorities, CI stakeholders (operators, administrators), SMEs, research and academia and society. The effects of using this service can be two-fold. If the question is pertinent with the CIPRNet aims and scope, end-users will receive a short answer by the CIPRNet expert and/or links to publicly available sources (if this is justifiable in the context of a given question). For more complex questions, the requesting user will be put in contact with the most appropriate CIPRNet expert(s), selected from the pool of experts, based on the subject raised by the user.

The "Ask the Expert" service will incorporate a number of procedures to guarantee possible anonymisation of the query, to protect data and queries from being publicised (if requested) and to ensure the secure protocols for the authentication of the user.

The main functionalities of the service include:

- Requesting the information via a pre-formatted form (e.g. a form with such fields as: subject, description, domain type/name, etc.),
- Registration of request and its maintenance,
- Maintaining the database of experts providing the knowledge for the service purposes. Such database should contain at least the following information: expert status (available/non-available), contact info, domain of expertise, scope of the possible issues to be solved,
- Filtering of requests (e.g. to reject nonsense, out of the service scope, or too trivial requests, spam messages, etc.),
- Queuing (including storage of waiting requests with their status—e.g. solved, in progress, unsolvable, etc.) and sorting the requests based on category/topic,
- Distribution of particular requests to the most appropriate CIPRNet experts,
- Replying to the question by the expert,
- Safe storage of (anonymised) past questions and answers in order to:
  - Control the utilisation of experts,
  - Control the distribution of topics, themes and question categories,
  - Control the quality of service (e.g. issues unsolved vs. overall number of investigated issues),
- Building the repository of the frequently asked questions (FAQs) and answers to optimise the utilisation of expert resources (by an automatic reuse of the most relevant answer to a given frequently asked question),
- Privacy and security functions and settings, e.g. to define the anonymity level of a request, whether the query/request will be publicised and available for a wider audience, etc.

5.1.2 Input information

The main input information for this service will be the practical and theoretical knowledge of the CIP experts that will serve as a source of the CIP-related information and expertise. Additionally, resources collected for the CIPedia service (e.g. links to the CIP documents) could serve as background resources for the "Ask the Expert" capability, complementing the experts' answers.

5.1.3 Output information

The output information during the service operation will be:

- The experts' answers to the particular questions,
- A list of frequent (historical) questions and answers that the user can investigate (and find solution) before contacting the expert.

5.2 CIPedia© service

5.2.1 Description

CIPedia© is one of the means providing the innovation of the CIP domain by the CIPRNet project and is defined in D8.4 document (CIPRNet 2014). The main purpose and rationale for CIPedia© is the need for common understanding of the CIP-related context by the multi-disciplinary CIP community. Each member of this community can bring his/her view on particular CIP elements and share it. In this sense, CIPedia© will be the place in which different visions, definitions and points of view are mixed, in order to develop a common understanding of the CIP-related aspects. In result, CIPedia© will foster an international collaboration of experts from the CI domain and will improve the cross-communication and creative discussion between them. The main assumption is that CIPedia© will be a multinational, multidisciplinary and cross-sector tool for anyone seeking information on CI-related matters.

5.2.2 The role of the service

CIPedia© is the online knowledge repository, similar to other wiki-like services (such as the Wikipedia). CIPedia© will become one of the components of the CIPRNet's VCCC web portal (CIPRNet 2014).

The main characteristics of wiki-like services (thus also CIPedia©) include:

- Simplicity of content creation (using simplified mark-up language), moderation and maintenance,
- High usefulness, easiness of navigation and content searching,
- Openness for adding new content and improving the existing information.

The initial content provided by the service consists of a multi-sector and multi-disciplinary CIP glossary, developed during IRRIIS, DIESIS (Usov et al. 2010; Masucci et al. 2009), ERNCIP (ERNCIP 2015) and CIPRNet activities. This glossary has been converted into a wiki-like online service, currently being evaluated and improved by

the CIPRNet consortium. On short term, it will be made readable to the public, and then open for write access to registered experts.

The target for CIPedia© are all groups of CI stakeholders, including policy-makers, relevant authorities, CIP operators and owners, manufacturers, CIP-related facilities and laboratories, and the society. CIPedia© is also a community-building instrument. Experts in CIP and CI sector experts shall be encouraged to register at CIPedia© and make contributions to its contents. In a longer perspective, CIPedia© will contain also information on European and international CIP policies, links to main policy and regulatory documents, and more.

5.2.3 The key properties of the service

From the perspective of the CIPedia administration and maintenance, the service will allow for:

- Verifying the newly created accounts (including security verification, e.g. anti-botnet measures),
- Assigning the newly created accounts to the pre-defined groups of users (e.g. administrators, moderators, reviewers, standard users, etc.),
- Safe storage of the online identities owned by the registered users of the service,
- Safe storage and indexing of the online content (actual and backups of historical articles, articles discussed before verification, etc.),
- Organising the content in various (Wikipedia-like) categories. The specified categories (e.g. one for glossary, another for policies, law acts, etc.) will improve the usability of the service and improve the effectiveness of the navigation, while using the CIPedia©.
- Verifying, reviewing and (in result) accepting or not the user created content. Such mechanisms are necessary to maintain the reliability and trustworthiness of information generated by users. Other purpose of these functionalities is the security of users which should assure that e.g. external HTTP links placed in the article text will not redirect them to a malicious website,
- Tracing and logging the activities performed on content, as well as viewing the past versions of a given article, in order to restore it in the case of so-called "online vandalism".

The security-related functionalities result from the fact that both the CIPedia© and wiki services are focused on openness and allow the broad spectrum of users (often anonymous in terms of expertise, knowledge, intentions) to access. Therefore, mechanisms such as access control, verification of user-generated content and other security measures are essential to keep order and provide the quality of the collected content.

5.2.4 Input information

The initial contents of the CIPRNet CIPedia© service consists of the CIP glossary developed during the project by the CIPRNet consortium. Further CI-related knowledge shall be introduced to the repository as user-generated content.

5.2.5 Output information

Output information are Wiki-like pages and articles, organised in a structured manner and containing CIP-related knowledge and information.

6 Non-technical aspects of CIPRNet DSS services

There are a number of non-technical aspects that have to be taken into account when developing the CIPRNet DSS and before its services are launched. They concern the legal, organisational and long-term customer support issues.

The analysis of these aspects has been divided into two groups. Firstly, the aspects related to some specific conditions under which services will be deployed during the runtime of CIPRNet are described. Afterwards, general requirements for future EISAC services are provided.

During the CIPRNet project the aspects related to the legal, organisational and customer support will be addressed differently in contrast to typical commercial solutions aiming at business continuity, growth, and ravenous. It must be emphasised that CIPRNet is a research project and as such it may follow different (non-commercial) regulations and limitations when it comes to licences related to data sources (e.g. geospatial data), software components (e.g. libraries and software frameworks), and third party external services (e.g. Google maps). Typically, these licences allow the researches to use mentioned before resources freely without being charged. However, as far as access to data is concerned, the CIPRNet consortium will not offer/allow for access to any raw/input data we use, only aggregated data or the results will be provided. The handling of data is guided by CIPRNet's Ethics Guidelines. When it comes to the organisational and customer support, during the project CIPRNet lifetime, all aspects related to services maintenance, bug-fixing, and responsibilities management will be handled by organisations developing certain services or its components. It must be also mentioned that all services, being part of a CIPRNet proof of concept, shall clearly define terms of use. Therefore, the end-users must be appropriately acknowledged that they

use the services on their own risk without any warranty and their authors will not be liable for any damages arising from their use.

These aspects are related, in the first place, to some formal arrangements as regards the functioning of EISAC—what legal form it will take (of a company, non-profit organisation, association) and to the final form the DSS will take.

Establishing EISAC as a legal entity involves taking into account different legal aspects, as e.g. the intellectual property, liability, licensing, data collection, administrative legal overhead, sharing and protection and flexibility. The intellectual property protection may refer to EISAC as a legal entity and would thus, e.g. involve the protection of the name (trademark) that will be established for it. It may also refer to the products and services of EISAC. The CIPRNet DSS will contain data, information, software or other items coming from external entities. Care has to be taken to sign appropriate contracts with each of them. E.g. the input data to the DSS (data registries, pieces of software) will come from different sources. Each time a new data source is planned to be added to the system, the license conditions for the use of the data need to be checked with the owner of the data source. Some sets of data (or software) will be free of charge but, still, an agreement for using them may be needed. Some other ones will have to be paid for and the payment might be one-time or recurring. The licenses might be periodic (even if long-term) and so the procedures have to be installed in order to check the validity of a given license and, if needed, to prolong it.

Some input data coming from external sources may not be licensed but a permission to use it will have to be granted. Such copyright issues will have to be checked when the DSS will use the publications, research results, data on CI, etc., coming from external bodies. Likewise, copyright and terms of use of all EISAC materials/products should be defined and communicated to the users, in case it should be used by them for their own purposes (e.g. for research). This approach (of checking the licenses/copyrights issues) should be applied for all the items that will form part of the CIPRNet DSS. This will ensure EISAC holds the rights to the DSS and its all services.

The names of the products and services should be carefully chosen and registered. It has to be remembered that the new EISAC services/products/inventions should be checked as whether they could be patented.

In case there are consolidated data in the system, e.g. the licensed one with not-licensed, the data filtration feature should be provided (filtration by rows and attributes), for the users not having the license to use a particular data source (attributes). Different access levels should be defined in the system, in order to reflect the user privileges and licenses—some content will be restricted to some users. This should be followed by providing different graphical user interfaces (GUI) for those different access rights.

The end-users will be asked to share their private data, and so the privacy-related aspects have to be dealt with when designing, developing and then using the CIPRNet DSS. The provisions of the EU directive 95/46/EC (European Parliament and Council 1995) have to be respected. This directive regulates the processing of personal data within the European Union, specifying the rules for data collecting, storing and using. The end-users should be aware of which data they are providing is being stored in the system and for what purpose. Data should then be used only for that specific purpose. The system provider should secure the users' personal data and should not disclose it without their consent. The users should be given the information as to who is collecting their data and they should have access to their data and be able to modify or delete it. A privacy policy should be defined for all services within the DSS and the users should accept it prior to using the service.

The taxation issues should also be considered (who is required to pay taxes, in which circumstances etc.)—they should be regulated by the law in force in the country of operation of a given provider.

For each service available in the DSS different service level agreements (SLA) should be established for those using the service. The SLA should be different for different client types etc. The payment policies should also be established—they should be the same for all services. The terms of use of the services should be specified and they should probably be the part of the SLA (specifying the party responsible for wrong decisions etc.).

It is important to have a clear vision of who will be the owner of the CIPRNet DSS and what will be the responsibilities related to providing the DSS services, which may be decided on when a legal form for EISAC is agreed on. The system could be owned by EISAC that would have the coordinating role as regards the operation of the system. EISAC local representatives (e.g. in Italy, Germany) would be responsible for the operation of a given local system—they would have the system translated into local languages and they would be providing the services, dealing with data providers and users, maintaining the system etc. The questions related to the ownership of the system and the relations between the EISAC and the local EISAC bodies should be clearly defined. Specific aspects important in this regard are: data management, data security, database maintenance, license procurement, and SLA negotiation.

All legal issues related to the responsibilities of local EISAC bodies should be decided on in accordance with the local law regulations.

One other non-technical issue that has to be taken into account when planning the CIPRNet DSS is the long-term customer support. Several issues related to this will have to be dealt with. Some of them concern the development phase, e.g. bug-reporting and solving and developing new features (who will pay for them). Long-term customer support also embraces issues related to infrastructure—who will pay for which part of it (hardware and software), how will the maintenance be dealt with, when should the hardware and software be replaced and who will cover the costs etc.

7 Conclusions

In this paper we described the set of services composing the decision support system for CIP and CIPRNet Virtual Centre of competence and expertise in CIP.

We also showed our approach in which the services design was strongly motivated by stakeholders needs and expectations. Therefore, the proposed services are expected to improve effectiveness of CIP decision makers.

Particularly, the threat visualization, forecasting, and consequences analysis services will allow the end-users to deal with constantly changing information during CI crisis and to more effectively build the reliable view on crisis situation. The What-if analysis service will allow users to examine various crisis scenarios (in order to explore different courses of action) and to learn about results of various possible decisions. Moreover, the CIPedia© and "Ask the expert" services will constitute the basis for the CIPRNet project centre of competence and expertise providing the innovation in the CIP domain.

Concluding, the presented results and our approach will prepare the basis for the EISAC.

Acknowledgments This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450. The European Commission's support is gratefully acknowledged. The work is also funded by Polish National Centre for Research and Development (NCBiR) from funds for science in the years 2013–2016 allocated for the international projects. Authors warmly acknowledge the work, in terms of ideas and practical implementations, of a number of colleagues of the different institutions involved: for ENEA, Antonio Di Pietro, Alberto Tofani, Maurizio Pollino, Luigi La Porta, Luisa Lavalle and Gregorio D'Agostino. For UTP Rafał Renk and Witold Hołubowicz. For Fraunhofer, Andrij Usov and Jingquan Xie. For JRC Christer Pursiainen and Naouma KourtiFor TNO, Eric Luiijf and Marieke Klaver. For Deltares, Annette Zijderveld and her team. For CEA, Dominique Sérafin and his team. For UCBM, Roberto Setola and his team. For UIC, José Pires and his team. For UCY, Elias Kyriakides and his team. For UBC, José Martí. For ACRIS, Bernhard Hämmerli and Marit Blattner.

Conflict of interest The authors declare that they have no conflict of interest. The funding is mentioned in Acknowledgments.

Compliance with ethical standards This work complies with the ethical standards.

References

CIPRNet (2014) Deliverable D8.4: Publicly Announced CIPedia. See also http://www.cipedia.eu. Accessed 22 May 2015

CIPRNet (2015) CIPRNet project website http://ciprnet.eu/summary.html. Accessed 22 May 2015

ERNCIP (2015) ERNCIP project platform, http://erncip-project.jrc.ec.europa.eu/. Accessed 22 May 2015

European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

European Parliament and Council (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Accessed 22 May 2015

Gartner Inc. (2011) Gartner says solving 'big data' challenge involves more than just managing volumes of data http://www.gartner.com/newsroom/id/1731916. Accessed 22 May 2015

Masucci V, Adinolfi F, Servillo P, Dipoppa G, Tofani A (2009) Ontology-based critical infrastructure modeling and simulation. Critical infrastructure protection III. Springer, Berlin Heidelberg, pp 229–242

Rome E, Bologna S, Gelenbe E, Luiijf EH, Masucci V (2009) DIESIS: an interoperable European federated simulation network for critical infrastructures. In: Proceedings of the 2009 SISO European Simulation Interoperability Workshop, Society for Modeling and Simulation International, pp 139–146

Usov A, Beyel C, Rome E, Beyer U, Castorini E, Palazzari P, Tofani A (2010) The DIESIS approach to semantically interoperable federated critical infrastructure simulation. In: Advances in System Simulation (SIMUL), 2010 Second International Conference, IEEE, pp 121–128