Cross-border Information Sharing for Critical Infrastructure Resilience: Requirements and Platform Architecture

Boris Petrenj
Politecnico di Milano, School of Management, Italy
boris.petrenj@polimi.it

Mariachiara Piraina
Politecnico di Milano, School of Management, Italy
mariachiara.piraina@polimi.it

Giada Feletti
Politecnico di Milano, School of Management, Italy
giada.feletti@polimi.it

Paolo Trucco
Politecnico di Milano, School of Management, Italy
paolo.trucco@polimi.it

Valentina Urbano,
Aria S.p.A., Lombardy Region, Italy
valentina.urbano@ext.ariaspa.it

Stefano Gelmi
Aria S.p.A., Lombardy Region, Italy
stefano.gelmi@ariaspa.it

ABSTRACT

Resilience of Critical Infrastructures (CI) is high on the agenda of countries' efforts. Modern CI are highly interdependent and span countries, so disruptions occurring on one side of the border can significantly affect economic and social functions on the other. To build CI resilience, stakeholder organizations must collaborate and exchange information throughout the Emergency Management (EM) cycle. In this paper, we present the *Critical Infrastructure Platform (PIC* in Italian*)*. PIC is a technological piece of a broader cross-border regional resilience strategy between Lombardy Region (Italy) and Canton Ticino (Switzerland) aiming to improve the capacity to manage accidental events involving transportation CI between the two countries. The main goal of the PIC platform is to support secure and effective information-sharing, inter-organizational risk assessment, monitoring and operational coordination under critical situations. The paper presents the key requirements of such ICT system, its high-level architecture including the description of its main modules, main takeaways and future steps.

Keywords

Critical infrastructure, interdependencies, resilience, cross-border, information sharing, IT platform, GIS.

INTRODUCTION

Contemporary societies are increasingly dependent on the availability of services provided by Critical Infrastructure (CI). Modern infrastructures have become highly interconnected, due to the increased flow of data, goods, people, energy, between CI sectors. CI assets do not operate in isolation but rather as a 'system of systems' where failure of one structure could result in serious disruptions in others (Lewis and Petit, 2019). This means that a single operator may have the best possible protection against direct hazards and threats and still have its operations and services disrupted due to the cascading effects, i.e. propagation of impact due to infrastructure

interdependencies. Even minor disruptions now easily cause service interruption in dependent infrastructures causing significant overall impacts, which must be considered on the system level.

In wake of a broadened range of hazards and threats which span across borders due to their spatial dimension (earthquakes, fires, severe weather, floods), it is also CI interdependencies that transmit impacts across sectors and across countries. It has become clear that CI stakeholder organizations cannot operate in isolation and must work together to ensure CI resilience, which became a shared responsibility between government and the private sector (Trucco and Petrenj, 2017). The increasing complexity of disruptions requires a collective (multi-agency, cross-sectoral and cross-border) approach in all risk management phases, where each actor benefits from connectivity, from sharing information and collaboration. In the efforts to build the resilience of CI systems, countries are working to establish mechanisms for information sharing, involving CI operators and other stakeholder organizations. Their aim is to establish a comprehensive and shared understanding of risks and vulnerabilities and coordinated emergency response, while ensuring the security and confidentiality of information shared. Numerous programs and approaches have been developed to foster trust-based connections between government and private owners and operators (OECD, 2019). The major (continental) initiatives fostering cross-regional and cross-country collaboration around CI systems include: *The European Union's Critical Infrastructure Warning Information Network – CIWIN* (EC, 2021); *United States Information Sharing and Analysis Centers – ISACs* (US DHS, 2016); *Canada Critical Infrastructure Gateway* (Government of Canada, 2020); *Australia's Trusted Information Sharing Network for Critical Infrastructure Resilience – TISN* (Australian Government, 2020); *South-America PROSUR* (PROSUR, 2020).

In European context, CI often span across countries, and there is a high level of heterogeneity of the involved organizations (data, technologies, procedures, organization, regulation, etc.), making it extremely difficult to exchange information and collaborate. "*All disasters are local*" (Serino, 2011), or at least start locally, and this is the principal level at which resilience is built. However, when a disaster hits, the neighbors will feel the impact too, and often be among the first responders.

In this paper, we present the *Critical Infrastructure Platform* (*PIC* in Italian), which is being developed within the SICt project (*Resilience of Cross-Border Critical Infrastructure*) which aims to improve the capacity to manage accidental events involving the transportation CI between Lombardy Region (Italy) and Canton Ticino (Switzerland). The goal of the *PIC Platform* is to support building cross-border regional resilience by supporting the cross-border coordination and decision-making, both in emergencies and in times of normal operation. The PIC will achieve this by encouraging end enabling secure information sharing to break down the boundaries between the stakeholder organizations. It will establish the cross-border information flows that are currently missing, but are necessary for: understanding of infrastructure vulnerabilities caused by interregional interdependencies; assessing criticality of specific infrastructure assets/facilities; estimating consequences of disruptions under specific scenarios; identifying risk-based and cost-effective mitigation options; and for coordinated incident management. For instance, the possibility to analyze and share information on how an emergency event (e.g. railway accident), occurring close to the border, will affect the traffic in both countries is useful to rapidly put in place adequate countermeasures. A collaborative approach would also allow for more effective management of the available resources, for coping with the emergency, securing the continuity of services and for limiting cascading effects.

The paper is structured as follows. In the following section, we give a brief state-of-the-art review of cross-border resilience, highlighting the gaps and the problem we are addressing. The methodology section explains the steps we have made to collect and analyze the requirements for the PIC platform. We then present the PIC platform by means of the requirements for cross-border information sharing, the high-level platform architecture and description of its internal and external modules. The paper ends with the main conclusions, limitations of the work and future developments.

CROSS-BORDER RESILIENCE

Much of the research in the fields of communication and information sharing for emergency management has focused on practices and training of key emergency management organizations, such as first responders (e.g. IN-PREP, 2021). In contrast, there has been little empirical investigation of the communication and information-sharing which would include CI operators (Reilly et al., 2018). Involving CI systems is relevant not only due to their importance for the normal functioning of societies but usually continuous CI operation is required during disasters to fully enable recovery activities and respond to community needs. However, during disasters the service capacity of many CI is knocked down. An unaddressed issue is certainly the need for synchronized information flows and shared situational awareness, especially when the impact spans across borders (Adrot et al., 2018).

When countries share CI and supply chains (including food, water, fuel and medical supply chains), disruptions

coming from one side can significantly affect economic and social functions on the other. The EC recognized that cross-border dimensions of risks could benefit from a more systematic assessment (EC, 2017). National risk assessments coordinated by the European Commission (EC, 2019) again revealed that while cross-sectoral interdependencies of risks are tackled to some extent, the cross-border/regional/international dimension is still missing. There has been significant effort dealing with cross-border Disaster Risk Reduction (DRR) and Climate Change Adaptation (CCA), including cross-border flood management, wildfires, and extreme weather (e.g. Abad et al., 2018; Bracken et al., 2016; EU-CIRCLE, 2021; Murphy et al, 2016;), but limited with transboundary infrastructure resilience. An overview of European programs and projects devoted to resilience is given by Adrot et al. (2018).

When it comes to cross-border coordination, another gap is that prior research and development effort has been mostly focused on the response phase of emergency/crisis, while it should cover each stage of the Emergency Management (EM) cycle and should be further enhanced in preparedness and risk mitigation phases (EC, 2020). Rather than designing systems for (cross-border) crisis management only, we should design systems that will function during both anomalous and routine operations (Allen et al., 2014).

Over the last decade, there has been an expansion of Public-Private Collaborations (or 'Public-Private Partnerships') with a goal of improvement of Critical Infrastructure Resilience (CIR) and Emergency Management (EM) all over the world (Trucco and Petrenj, 2017). In the US there has been a growing focus in developing cross-sector, multi-jurisdiction, and discipline partnerships to identify and address resilience gaps, and most recently on "operationalizing" resilience (Fisher et al., 2018). One of the first initiatives was developed in the Pacific Northwest Economic Region (PNWER) starting in 2001, to address regional cross-border infrastructure interdependencies (and potential disruption consequences) between the US and Canada. The development of a regional alert and warning system named 'Northwest Warning, Alert and Response Network' (NWWARN), encouraging cross-sector information sharing, was among the PNWER's major achievements. On the national scale, the "*Canada-U.S. Action Plan for Critical Infrastructure*" was designed to strengthen the safety, security, and resilience of CI, through an enhanced cross-border approach. The Action Plan identifies partnerships, information sharing, and risk management as the three key elements to better prevent, respond to, and recover from CI disruptions.

'Crisis Informatics' research combines social science and ICT knowledge to better understand how organizations and people use digital technology to better respond to disasters and crises (Karanasios et al., 2019). This field consists of many streams, and the focus of this paper is on developing and improving cross-border inter-organizational information sharing and collaboration, to improve the protection and resilience of CI. Timely, trusted information sharing and collaboration among stakeholders are crucial within the CIP and CIR mission (DHS, 2016). There are significant efforts to improve crisis and emergency situations focusing on the problems and significance of inter-organizational information sharing and collaboration (Allen et al., 2014). On top of numerous issues and barriers to inter-organizational information sharing and collaboration for CI resilience (Petrenj et al., 2013), cross-border CI dimension further increases the complexity of risk and resilience management. With different countries, regions, and agencies working together there are additional challenges associated with administrative and economic conditions, cultural and language barriers, systems in place, habits and social standards (Adrot et al., 2018; Bharosa et al., 2010). It seems that current methods and tools for collaborative networks are not fully suited to facilitate collaborations between different types of organizations in the crisis management domain. (Benaben et al., 2017). Emergency response plans and Incident Command Systems are well defined on the intra-organizational level, following organization's own hierarchy and resources, while, in reality, organizational units are forced to carry out tasks collaboratively (Noori et al., 2016).

(Inter-)Organizational resilience refers to the organizations that operate and manage the CIs, including the processes of organizational capacity and capability, planning, training, leadership, communication, and so forth (Rød et al., 2020). It is not a sole matter of an ICT system (technology) and its interoperability that would allow for efficient information sharing and collaboration, but it is a piece of a broader strategy dealing with inter-organizational resilience building. As CI operators might not always be inclined to share sensitive information about their vulnerabilities and critical dependencies outside of safe circles, ensuring mutual trust and security of shared information is an important aspect to foster a joint approach (OECD, 2019).

In this paper, we investigate the specific requirements of a collaborative environment that is necessary to facilitate collaboration for improved cross-border transportation system resilience. We are not aware of any common approach, technique or tool is available to enable continuously updated and shared information between organizations that would support the whole CI resilience management cycle, across agencies and across borders.

METHODOLOGY

The requirements for the cross-border information sharing platform (PIC) were collected from two main sources. On one side the experiences and expertise gained from the development and use of previous IT platforms for emergency management in the Lombardy Region was fundamental (e.g. Emergency Dashboard – *Cruscotto Emergenze* in Italian). On the other, the platform requirements specific for this new use case (cross-border) have been collected through SICt project workshops and interviews with the stakeholder organizations from both sides of the border. The steps followed to collect and analyze the requirements are the following:

1) Identification of stakeholder organizations. The identified groups were: road operators and police, firefighters, rail operators, medical emergency services operating in the geographical area of study.
2) Gathering requirements. Starting from September 2020, two workshops involving all the stakeholders have been organized in order to get the first set of high-level requirements. In addition, four cross-regional roundtables have been conducted gathering Italian and Swiss organizations in homogeneous groups (i.e. road operators and police, firefighters, rail operators, medical emergency services). A follow-up in the form of unstructured interviews has been conducted with individual organizations with the aim of understanding organization-specific requirements. In all these cases, there was continuous interaction between the interviewers (including at least a researcher and an IT expert) and the practitioner organizations, without adoption of a specific protocol, in order to favor an open discussion around the PIC requirements. The focus of these meetings was on the information needs (information flows and gaps) and on functionalities that could be introduced in the PIC platform to facilitate stakeholders' EM. In addition, the existing information systems in use were analyzed. The online meetings were recorded with the participants' permission, in order not to miss any detail and review without distraction what has been discussed.
3) Analysis of requirements. The requirements, previously collected in the form of summary lists, were analyzed by means of their clarity, completeness and possible conflicts. The requirements were then documented in a detailed report and shared with stakeholders. Moreover, the NATO Architectural Framework (NAF, 2018) was used as a standardized way of representing relevant viewpoints, such as the organizational structures and information flows.

The interviews are still ongoing and the requirements will go through a final revision before the PIC development.

PIC PLATFORM

This section describes the requirements collected for the development of the PIC platform and the proposed high-level architecture of the platform including the internal and external modules. The context of the platform application is the cross-border coordination between the Lombardy Region (Italy) and Canton Ticino (Switzerland) to build the resilience of the interconnected transportation network. The platform will be used to manage all types of incidents affecting the transportation infrastructure, regardless of the type of hazard (natural, man-made, technological).

Requirements for a Cross-Border Information Sharing IT Platform for CIR

Understanding the Current Situation

The analysis of the current situation focused on the information needs of the inter-regional stakeholders. The lack of an information-sharing tool for managing CI systems between the two countries was obvious.

The interviews with the stakeholders from both sides of the border revealed that inter-organizational communications were limited. The communication relied on personal relations, and were mainly performed using the telephone, and, in specific cases, email or radio. This is mainly because the telephone represents one of the quickest communication channels for emergencies. However, as stated by all the interviewed organizations, there are information that do not require a direct and synchronous interaction between people. For instance, a decision to close a section of the railway network can be communicated through a platform without using a telephone. Moreover, as highlighted in Figure 1, the major part of the cross-border communications is between first responders, which then forward the information to the other involved organizations. Still, there are plenty of cases where a direct (peer-to-peer) interaction between individual organizations would be beneficial. This stands for both emergencies and periods of normal operation, where risk assessment and emergency planning take place. An in-depth study (not included in this paper) identified the existing gaps in the information flows. It immediately revealed the absence of direct communication between the two states to communicate the occurrence of an event that affects a transport infrastructure system generating cascading effects on other systems. It means that the stakeholder organizations do not have proper access to all the external information they need for the best possible

risk and emergency management. Moreover, the cross-border exchange of information through an information system, as done by the rail operators, is much more efficient compared to the road operators' communication mediated by the police and done over a telephone. The interviews also pointed out that many operators do not have a geospatial platform to consult, and in addition, not all geographic data of interest are currently available. The PIC will therefore support a geographic representation of information and, the flow of missing data to the shared platform will be added.

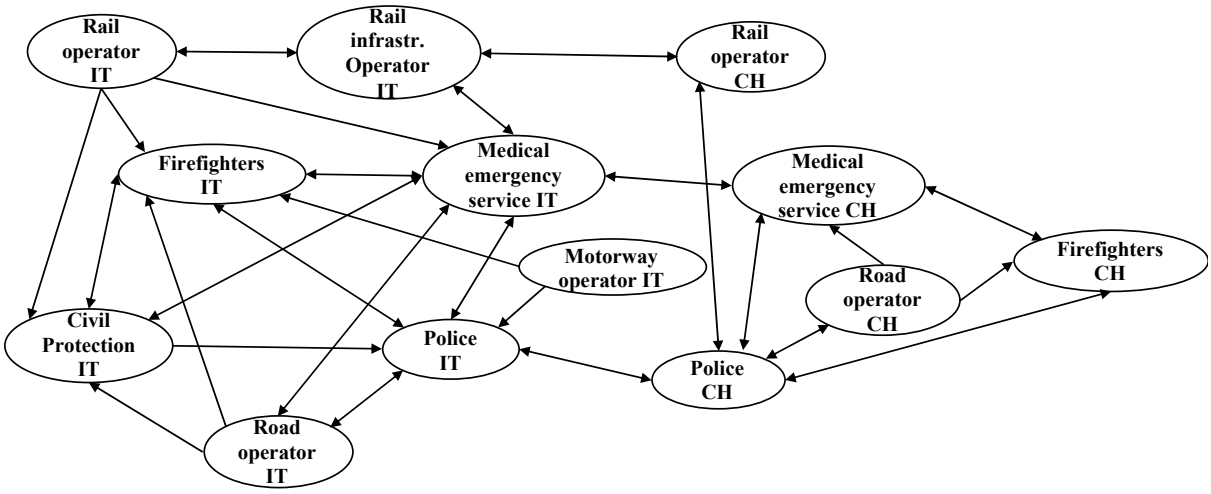

Figure 1. Existing information flows between the regional stakeholders

To address the gaps in the information flows we proceeded with the collection and definition of the PIC platform requirements, which is the first step of the system development process.

Functional Requirements

The functional requirements of the platform are divided in:

- General functionalities;
- Critical Infrastructure Dashboard functionalities;
- Collaborative Emergency Management functionalities;
- Mobility functionalities.

Considering the *General* functionalities of the platform, different user profiles are defined, each of them having specific permissions and access to different types of information, all according to the privacy requirements of the shared information. The current types include the configurator (high level), local administrators (mid-level) and general users (low level). The users that will have access to the platform include first responders, CI operators and public entities that operate in that geographical area. The users will be assigned to a specific group and each group will be characterized by a role. Belonging to a group gives the user the visibility of one or more scenarios – a specific set of information that can be viewed and consulted through the geographical interface (map) of the Critical Infrastructure Dashboard. The functionalities are linked to user groups, not scenarios.

The geographic component (i.e. *Critical Infrastructure Dashboard*) allows visualizing, consulting and interrogating data on a map. The presented data can be static or updated in real-time thanks to the possibility of PIC to collect data from some of the information systems of the users (stakeholder organizations), or get data inserted directly by users. For instance, there will be the possibility to have access to the contents of webcams owned by CI operators positioned in strategic locations, or to see the location of some resources owned by CI operators and first responders. As shown in Figure 2, by clicking on the webcam icon on the map it is possible to see all the layers of information associated with that icon (i.e. webcam locations with the corresponding images, the owner of the webcam, CI asset visualized in the images). Similarly, by clicking on the icons of resources owned by CI operators (e.g. railway stations, road segments) it is possible to have information about the status of the traffic. By interrogating resources owned by first responders (e.g. health facilities, police stations, firefighter stations) it is possible to get the address of the facilities and their contacts. Moreover, the alerting system will be associated with critical events on the map so that the user is immediately informed through alerts.

To favor *Collaborative Emergency Management*, there will be the possibility to use the platform as an information sharing system containing an address book, a messaging system and a document repository. This module will allow the possibility to manage events and alerts.

Mobility module will complete the platform through functionalities related to the analysis of the transportation system considering specific scenarios. It will provide information on the possible strategic measures to improve the resilience and/or actions to be taken in a specific scenario.
Finally, the functionality will include viewing and querying through the information and results of other connected modules (internal and external) – the integration requirements will assure their compatibility.

Figure 2. Geographic component of PIC

Information Requirements

The information requirements are related to all the information present in the geographic platform of PIC (i.e. critical infrastructure dashboard) and in the management part (i.e. collaborative emergency management module). By default, geographic services are made available through the *Critical Infrastructure Dashboard*, which will provide data related to the geographic area of the project, the road and the rail network (including the details of each designated transportation network node). Moreover, it will show the location of the resources, vehicles and assets of some stakeholders. This will be completed through the other modules that will suggest the actions to implement in order to improve the resilience of the system (e.g. simulation of the effects of an emergency event, traffic management, infrastructure accessibility).

Other Requirements

The functional and information requirements are completed through the architectural and integration requirements. They are related to the integration of the internal modules and the external systems that will provide useful information and analytics. The modules are presented in more detail in the following section of the paper. Moreover, the accessibility and compatibility with different browsers is guaranteed, together with the privacy requirements.

PIC Platform High-Level Architecture

PIC is a unique, shared platform for Italian and Swiss operators to access information and analytical tools, to share planning procedures in the preparedness phase and coordinate response actions during an emergency event.

The platform is being developed as a web application and it is composed of three internal modules with specific functionalities, as framed in Figure 3:

- Critical Infrastructures Dashboard;
- Collaborative Emergency Management Module;
- Mobility Module.

PIC Platform will be also integrated with external applications and systems, represented outside the red line in Figure 3, which are:

- Emergency Operations Room register and Alert Management;
- GRRASP-DMCI (suite for CI vulnerability and risk analysis jointly developed by EC-JRC and Politecnico di Milano (Galbusera et al., 2020);

- Infrastructures Monitoring Network;
- Applications and systems of operators and first responders.

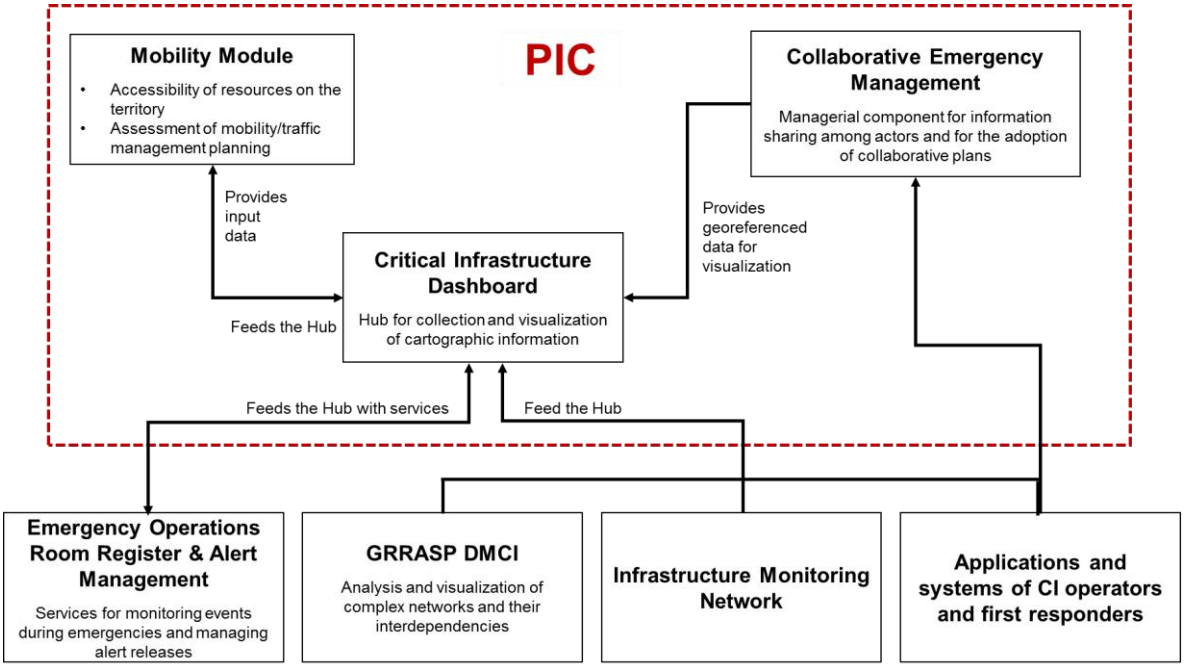

Figure 3. PIC platform architecture

Internal Modules and Legacy Systems

The internal modules inside PIC are based on legacy systems that were already in use by the regional government (e.g. *Emergency Dashboard*). They were improved and advanced according to the specific requirements of the project. Internal modules interact through uni or bidirectional flows of data.

Critical Infrastructure Dashboard (CID) is the component enabling the visualization and the cartographic analysis of all the information useful for operators. It represents the data collection hub of the platform and interacts with an Oracle/ArcSDE database which physically hosts data that cannot be made available through other services. It is the geographic component of PIC platform, therefore it will enable users to visualize, consult and interrogate data on a map. The CID is the core element of PIC, which will provide the Common Operation Picture by integrating and displaying all the relevant information in one place, and make it available to stakeholders on both sides of the border.

It will interact with other internal modules of the platform and with the external applications. More specifically, it includes:

- A bidirectional flow of data with Mobility Module. CID provides this module with input data to be processed, it receives the results of the processing and it represents them on a map;
- A unidirectional information flow from Collaborative Emergency Management module. CID can show the georeferenced message;
- A unidirectional information flow from Emergency Operations Room, GRRASP, Monitoring Network and Applications of operators and first responders. CID can show all the received data on a map.

The CID is the principal user interface and the first thing users see upon access to the PIC through authentication. The data that users can visualize within this module are:

- Presence of construction sites or traffic blocks;
- Road traffic;
- Rail traffic;
- Installations and sites: location of hospitals, first aid, fire stations and other relevant sites;
- Video surveillance;
- Mass and dimension limitations;
- Resilience indicators: resilience level of different segments of the road network. It could be further investigated to analyse the components that contribute to the aggregate resilience value.

Collaborative Emergency Management (CEM) module is an application component endowed with the following functionalities:

- Directory: it includes data and contact details of operators involved in the emergency management;
- Document repository: it allows saving documents and photos related to an event;
- Messaging system: it enables communication through real-time chat or emails. Users can create new message templates or use predefined ones. The module allows selecting the receivers of the messages (broadcast or selected group of users) and receive appropriate notifications.

CEM will also enable operators to insert new Alerts and Events, giving the possibility to associate to them all the related information, and support them in managing and coordinating response actions. An Alert is a warning that users receive to be prepared to deal with potential emergencies. Qualified users can create a new Alert by map editing of a point, a line or a polygon, or by selecting the affected road segment. Users proceed by inserting significant information related to the selected geometry or road segment in a template. The set of information characterizing an Alert is (information marked with a star is mandatory to create an Alert):

- Expected date*;
- Expected time*;
- Expected duration;
- Geolocation*;
- Phenomenon location: possibility of adding a description to the geolocation of the phenomenon;
- Phenomenon description*: possibility to select the type of phenomenon by a drop-down menu (Hydrogeological risk, Hydraulic risk, Severe thunderstorms, Snow, Avalanches, Severe wind, Fires, Other) and to specify the expected magnitude;
- Reporting operator*.

On the other hand, an Event is any happening that could undermine the functionality of the CI and that requires an intervention of operators to be managed. An Event generation can be triggered by an unforeseen accident or it could result from an escalation of an Alert into an emergency. Qualified users can create a new Event by map editing a point, a line or a polygon, or by selecting the affected transportation node. In particular, CI operators can create a new Event when it is located on a road/rail segment within their competence. Users proceed by inserting relevant information in a template. The set of information characterizing an Event is (information marked with a star is mandatory to create an Event):

- Date*;
- Time*;
- Geolocation*;
- Event location: possibility of adding a description to the geolocation of the Event;
- Event description*: possibility to select the type of Event by a drop-down menu;
- Reporting operator*;
- Expected duration;
- Event status: possibility to associate the Event status by a drop-down menu (Open or Closed).

It will be possible to further detail an Event by activating different templates, whenever new information emerges and new measures are implemented. Additional information that could be relevant for users, since it supports them in managing emergencies, are listed in Table 1. Knowing the details about events happening on one side of the border can help operators on the other side in implementing actions to manage the propagation of the effects. Information is grouped in different categories, according to their nature:

- Event features: operators will have the possibility to insert information, to update information already entered or to share new details;
- Response actions to respond to the event;
- Recovery actions: measures and resources put in place by operators to restore CI conditions to normal.

Operators will also have the possibility to declare their state of emergency if an ongoing event requires their intervention, and finally, to notify about the closure of an event.

Mobility Module is an application component linked to the transport domain. It is based on processing that will suggest the measures to implement in order to improve the resilience of the CI system. On one hand, considering the available resources for managing a significant event, it aims at analysing resources accessibility on the territory. On the other, it aims at assessing plans and procedures for road and rail mobility/traffic management.

For instance, there will be the possibility to have information about alternative routings and to visualize them on the map.

Table 1. Additional information related to an Event

Event features	
Information	**Description**
Substances	Leaked dangerous substances within the area: • Flammable; • Toxic; • Radioactive; • Pollutants; • Other (to be specified).
Substance quantity	Quantity of substances leaked in the environment.
N° involved people	It includes deceased, injured, people to be evacuated, potential targets and isolated people.
N° injured	
N° deceased	
N° people to be evacuated	
Medical aid	It shows effects related to heath care, showing the main pathology of patients: • Traumatized; • Polytraumatized; • Burn victims; • Intoxicated; • Other (to be specified). Beside each pathology item, users will insert the estimated number of involved patients.
N° and type of vehicles involved on the road	It shows the types of involved vehicles: • Light vehicles: Car, Other (to be specified); • Heavy vehicles: Bus, Truck, Lorry, Other (to be specified). Beside each vehicle item, users will insert the estimated number of involved vehicles.
N° and type of wagons involved on the rail	It shows the types of involved wagons: • Freight wagon; • Passenger train; • Other (to be specified). Beside each wagon item, users will insert the estimated number of involved wagons.
Response/recovery measures	
Information	**Description**
Restriction on transit of heavy vehicles	It displays potential restrictions on transit of heavy vehicles and supports operators in managing the areas used to store this category of vehicles.
Restriction on transit of light vehicles	It displays total or partial restrictions on transit of light vehicles.
Restriction on transit of train	It displays potential blocks of rail traffic.
Variable message sign	It offers visibility on the position of variable message signs and the possibility for the operators to add the relative text.
Request of support	It allows operators to ask for support in case of need.

External Applications

External applications are already existing systems used in other contexts, which are able to process and return information of interest for the PIC platform users. The selection of these systems was made taking into consideration the insights and benefits they could bring in, but also the feasibility of their integration with PIC platform.

Emergency Operations Room (EOR) Register is an application currently used by the Civil Protection of Lombardy Region for monitoring of events during emergencies. The service is reserved to the General Directorate responsible for Civil Protection, to operators of the EOR and to the members of the Regional Crisis Unit. It enables to access or upload information related to events involving Civil Protection at the local, provincial, regional and

national level.

The EOR Register includes information about Events, Alerts, Warnings and Criticality level in the EOR (absent, ordinary, moderate, high, emergency). It supports users in managing actions to be undertaken and requests of activities.

Alert Management (GESTCOM) includes a set of services for configuration, generation and multichannel delivery of alerting releases from Functional Risk Monitoring Centre – Civil Protection RL. Alerting status managed through GESTCOM is analogous to those described in the EOR Register.

The *Dynamic Functional Modelling of vulnerability and interoperability of Critical Infrastructure* (GRRASP-DMCI) is a discrete event simulation that analyzes the dynamic behavior of the CI system-of-systems as a result of a threat impacting one or more infrastructure nodes. DMCI objective is to develop knowledge about how disruptive events or disturbances acting on CI could spread to the whole network because of different types of interdependencies and affect businesses, end-users and the entire society. The first DMCI model (Trucco et al., 2012) was enhanced in recent years and integrated into the *Geospatial Risk and Resilience Assessment Platform* (GRRASP) developed by the JRC (Galbusera and Giannopoulos, 2016). The latest version of the model (DMCIe; Galbusera, et al., 2020) is currently being used for the needs of the SICt project.

The DMCI model had been previously applied to analyze the wider EXPO 2015 area in Milan (Italy); critical scenarios analysis and evaluation of resilience strategies (Petrenj and Trucco, 2014); supported regional decision-makers in evaluating transportation unlock policies in the metropolitan area of Milan during COVID-19 contingency (Trucco et al., 2020); for Vital Node Analysis (VNA) in the SICt project.

GRRASP combines geospatial technologies and computational instruments for complex network analyses, with the aim of identifying functional, geographical and logical interdependencies among the different network components. More specifically, the purposes are:

- To simulate potential impacts on interdependent CIs following an emergency situation and plan procedures of intervention in advance;
- To support operators' activities during emergency events, providing information about the impacts and the potential propagation of the disservice.

GRRASP can be used for analyses of CI interruptions at local, regional, national and international level. Functionalities of GRRASP will be available through its integration with the PIC platform, without further authentication. The system will be prepared and pre-populated with a master dataset that contains the following information:

- Identification of critical nodes of transport cross-border CI. Information about nodes and their descriptive parameters are gathered by both available public data and direct collection from operators of specific nodes;
- Vulnerability and nodes interdependence analysis, with standardization of analytical criteria of judgement between the two countries. Static and dynamic parameters will be used to describe the characteristics of each CI node and they will lead to defining vulnerability levels, referred to a standardized scale, for each threat and hazard affecting the node itself.

CI operators will be able to use the pre-populated dataset for processing and personalised analyses about CI nodes interdependencies, thus creating their own project.

Infrastructures Monitoring Network

SICt project will include the implementation of an Infrastructure Monitoring Network. Decisions related to the typology of instruments to be used for monitoring are still in progress, however, the data that will be received by the PIC platform are the following ones:

- Satellite images;
- Images from drones;
- Frame videos from drones and cameras.

For satellite images, radar data acquisition will be programmed with a frequency of 36 days. The collected data will be the input for interferometric processing, whose results will enrich the information asset of PIC.

Applications and Systems of Operators and First Responders

Operators and first responders involved in the project currently use their own applications and systems to manage

emergencies and to store geographical data not related to specific events. Where possible, the data included in Table 1 will be made available and shared within the PIC platform.

Key Technical Details

The technology behind the PIC platform will be: Tomcat lispa 3.9.1, Open JDK 13, Esri API Javascript and Esri ArcGIS server. All modules will be implemented via Web-Application and the databases (DB) used will be different according to the considered modules. Concerning the geographical component, CID will be mainly a service collector and the few data physically available will be collected in an Oracle/ArcSDE 10.8 DB. On the other side, CEM will have an Oracle 18c DB.

To guarantee data security, the access to the PIC platform will require authentication by both Italian and Swiss users. Furthermore, most of the data will be provided to PIC through services, while for the data contained in the DBs, the data security rules will be the ones provided by the DBs themselves.

CONCLUSIONS

The present work fills the gap in the wider literature by providing the empirical investigation on the information requirements for improved cross-border risk and resilience management of networked CI systems. Firstly, there has been little analysis that involves CI operators among the key stakeholders. Secondly, there is a lack of focus on CI in the context of cross-border resilience (compared to DRR and CCA). Finally, the previous efforts mainly tackled information sharing in the emergency response phase rather than covering all resilience capacities (phases).

The study starts from the acknowledgement of the importance of collaboration and information sharing as the key capability for improving the resilience of CI systems. This is particularly relevant when dealing with cross-border CI disruptions and related cascading effects. This paper provided an overview of the PIC IT platform for information sharing that is being developed in the context of the SICt project, where CI operators, first responders and governmental institutions from Italy and Switzerland are involved. The development and implementation of this kind of cross-border information system presents one of the key steps towards building resilience capabilities between the two countries. The PIC responds to the need for an integrated cross-border system that would allow covering the information sharing issues and gaps in all EM phases. Different modules, providing specific functionalities, are integrated into one common platform. The modules acquire information directly from the systems that operators currently use, without requiring additional effort from their side. The presented architecture of the PIC platform, as well as the functionalities of each module, are still a work in progress and subject to changes based on the testing and end-user feedback upon the first release.

The main technical challenge is the integration of the information coming from the existing IT systems in use by different stakeholders. The social dimension brings challenges such as differences in terminology (even though the Italian language is spoken in both regions). The previous phases of the project have also revealed differences in the standards for the classification of natural hazards, and in metrics used to express their probabilities and magnitudes. An open issue inside the PIC requirements is the management of related ('father-son') events, for example in cases when an event causes another event, or when an event is caused by a combination of two father events.

Resilience planning cannot be done without having the key stakeholders connected and enabled to securely and trustfully share information. In this regard, an IT platform is not the solution on its own, but the enabler of a collaborative process between organizations. Hence, even though the PIC presents a considerable step forward, as one of the key elements for building cross-border resilience, it must be accompanied by proper inter-organizational arrangements and collaborative models to achieve its full potential and effective exploitation. A major hurdle for cross-border incident management, and resilience building in general, remains the unfeasibility of cross-border response. This kind of response would require a cross-border movement of resources, some of which might be prohibited, such as firearms or medicaments, and movement of personnel, which raises regulatory issues of responder training, liability and insurance. Tackling these issues would require national-level support through coordinated national CI resilience policies with neighboring countries and beyond, and development of cross-border assistance mechanisms.

ACKNOWLEDGMENTS

The work described in this paper is developed as part of EU project 'Sicurezza delle Insrastrutture Critiche transfrontaliere - SICt' which is co-funded under Interreg V-A Italy-Switzerland Cooperation Programme 2014-2020.

REFERENCES

Abad, J., Booth, L., Marx, S., Ettinger, S. and Gérard, F. (2018). Comparison of national strategies in France, Germany and Switzerland for DRR and cross-border crisis management. *Procedia engineering*, *212*, 879-886.

Adrot, A., Fiedrich, F., Lotter, A., Münzberg, T., Rigaud, E., Wiens, M., Raskob, W. and Schultmann, F. (2018). Challenges in establishing cross-border resilience. In *Urban Disaster Resilience and Security* (pp. 429-457). Springer, Cham.

Allen, D. K., Karanasios, S. and Norman, A. (2014). Information sharing and interoperability: the case of major incident management. *European Journal of Information Systems*, *23*(4), 418-432.

Australian Government. Department of Home Affairs (2020). *Trusted Information Sharing Network (TISN)*, Critical Infrastructure Centre. Retrieved from https://cicentre.gov.au/tisn

Benaben, F., Montarnal, A., Truptil, S., Lauras, M., Fertier, A., Salatge, N. and Rebiere, S. (2017, January). A conceptual framework and a suite of tools to support crisis management. *Proceedings of the 50th Hawaii International Conference on System Sciences*

Bharosa, N., Lee, J. and Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises, *Information Systems Frontiers, 12*, 49–65.

Bracken, L. J., Oughton, E. A., Donaldson, A., Cook, B., Forrester, J., Spray, C. Cinderby, S., Passmore, D. and and Bissett, N. (2016). Flood risk management, an approach to managing cross-border hazards. *Natural Hazards*, *82*(2), 217-240.

EU CIRCLE Project (2021, April). Retrieved from http://www.eu-circle.eu/

European Commission (2017). Commission Staff Working Document: Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final

European Commission (2019). Recommendations for National Risk Assessment for Disaster Risk Management in EU, JRC Science for Policy Report

European Commission (2020). *Prevention and Preparedness for Cross-Border Risks*, Funding & tender opportunities portal.

European Commission (2021, April). Critical Infrastructure Warning Information Network (CIWIN). Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

Fisher, R., Norman, M. and Peerenboom, J. (2018). Resilience History and Focus in the USA. In *Urban Disaster Resilience and Security* (pp. 91-109). Springer, Cham.

Galbusera, L. and Giannopoulos, G. (2016). *Re-engineering of GRRASP to support distributed and collaborative analysis of critical infrastructures*. Luxembourg: EUR 28072 EN, Publications Office of the European Union. https://doi.org/10.2788/450351

Galbusera, L., Trucco, P. and Giannopoulos, G. (2020). Modeling interdependencies in multi-sectoral critical infrastructure systems: Evolving the DMCI approach. *Reliability Engineering & System Safety*, *203*, 107072.

Government of Canada (2020). *Critical Infrastructure Gateway*, Public safety Canada. Retrieved from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx

IN-PREP Project (2021, April). Retrieved from https://www.in-prep.eu/

Karanasios, S., Cooper, V., Balcell, M. P. and Hayes, P. (2019, January). Inter-organizational collaboration, information flows, and the use of social media during disasters: a focus on vulnerable communities. Proceedings of the 52nd Hawaii International Conference on System Sciences

Lewis, L. P. and Petit, F. (2019) Critical Infrastructure Interdependency Analysis: Operationalising Resilience Strategies. Argonne National Lab, IL (USA)

Murphy, C., Creamer, C., McClelland, A. and Boyle, M. (2016). The value of cross border emergency management in adapting to climate change. *Borderlands: The Journal of Spatial Planning in Ireland*, *5*, 34-46.

NAF (2018). NATO Architecture Framework Version 4.

Noori, N. S., Wolbers, J., Boersma, K. and Vilasís-Cardona, X. (2016, May). A Dynamic Perspective of Emerging Coordination Clusters in Crisis Response Networks. In *ISCRAM*.

OECD (2019), *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris

Petrenj, B., Lettieri, E. and Trucco, P. (2013). Information sharing and collaboration for critical infrastructure resilience–a comprehensive review on barriers and emerging capabilities. *International journal of critical infrastructures*, *9*(4), 304-329.

Petrenj, B. and Trucco, P. (2014). Simulation-based characterisation of critical infrastructure system resilience. *International Journal of Critical Infrastructures*, *10*(3-4), 347-374.

PROSUR (2020) Annual Work Plan 2020-2021, Thematic Area: Disaster Risk Management and Resilient Development. Retrieved from https://foroprosur.org/wp-content/uploads/2020/11/GRD_Anual_Workplan_2020-2021_ING.pdf

Reilly, P., Serafinelli, E., Stevenson, R., Petersen, L. and Fallou, L. (2018). Enhancing critical infrastructure resilience through information-sharing: recommendations for European critical infrastructure operators. In: Chowdhury, G., McLeod, J., Gillet, V.J. and Willett, P., (eds.) Transforming Digital Worlds. *iConference 2018*, 25-28 Mar 2018, Sheffield, UK.

Rød, B., Lange, D., Theocharidou, M. and Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. *Journal of Management in Engineering*, *36*(4)..

Serino R. (2011). FEMA Deputy Administrator Richard Serino's keynote speech at the International Association of Emergency Managers (IAEM) Annual Conference, Nov. 14, 2011, Las Vegas (USA).

Trucco, P., Cagno, E. and De Ambroggi, M. (2012). Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engineering & System Safety*, *105*, 51-63.

Trucco, P. and Petrenj, B. (2017). Resilience of Critical Infrastructures: benefits and challenges from emerging practices and programmes at local level. In *Resilience and Risk* (pp. 225-286). Springer, Dordrecht.

Trucco, P., Maggia, P. and Petrenj, B. (2020, November) Adapting public transport to COVID-19 contingencies: evaluating unlock policies in the metropolitan area of Milan through DMCI simulation. *Proceedings of ESREL2020 PSAM15.*

United States. Department of Homeland Security (2016) *Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community*, US Department of Homeland Security