A Semantics-Based Common Operational Command System for Multi-Agency Disaster Response

Linda Elmhadhbi[1], Mohamed-Hedi Karray[1], Bernard Archimède[1], Neil Otte[2], and Barry Smith[3]

[1]University of Toulouse, INP-ENIT, Tarbes 65000, France

[2]University of Michigan, Michigan 48109, USA

[3]University at Buffalo, New York 14203, USA

linda.elmhadhbi@enit.fr

Abstract

Disaster response is a highly collaborative and critical process that requires the involvement of multiple government agencies and emergency responders (ERs) ideally working together under a unified command to enable a rapid and effective operational response. Following the 9/11 and 11/13 terrorist attacks, and the devastation of hurricanes Katrina and Rita, it is apparent that inadequate communication and a lack of interoperability among the ERs engaged on-site can adversely affect disaster response efforts. Within this context, we present a scenario-based terrorism case study to highlight the challenges of operational disaster command and response. In this work, which is based on the French emergency response doctrine, we introduce a semantics-based common operational command system that is designed to guarantee an efficient information flow among ERs. In particular, our focus is on offering to all ERs a real-time operational picture of the situation in order to enable multi-level coordination among firefighters, police, gendarmerie, healthcare units, public authorities, and other stakeholders. Our approach consolidates information in order to promote timely sharing among ERs. The proposed system is based on an ontology that has been developed to represent the different types of knowledge on the part of ERs, providing a shared vocabulary that covers a variety of interoperability concerns arising for example because data are collected in different formats, because the different functions of different stakeholders are not taken into account, and because there are failures of coordination among different groups of emergency responders.

Index Terms— Disaster management, Command and control systems, Interoperability, Common language, Ontologies.

Managerial relevance statement

We propose POLARISC, a software solution that plays the role of mediation among all the ERs to support multi-agency operational management of disaster response. It is a semantically driven operational command system based on the French emergency response processes. In particular, it provides a set of services that enable offering to all ERs an appropriate and intelligible common operational picture of what is happening exactly on the disaster site, consolidating information and ensuring semantically interoperable communication among the involved stakeholders, improving the victims' evacuation process by enabling interoperability of data between the disaster area and the healthcare institutions, and enhancing the resource allocation process and their real-time tracking.

I. INTRODUCTION

Throughout history, disasters have caused the loss of human life and property damage that can directly or indirectly affect an entire nation. According to the US Department of Homeland Security National Response Framework, a disaster is any natural or manmade incident, including an act of terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions (Homeland Security, 2016). The need to face the suddenness, complexity, and the chaotic nature of disasters makes disaster management challenging (Devlin, 2006). The 9/11 and 11/13 terrorist attacks and the devastation wrought by hurricanes Katrina and Rita highlight the need to focus on improving disaster management. In the literature, research efforts have focused on improving disaster management by developing crisis information management systems (CIMSs). There are other terms used to describe software systems of this sort, such as disaster management interoperability systems and critical incident management systems. However, CIMS is the term most commonly used across multiple agencies and jurisdictions where information exchange and sharing and coordinated actions are required (Iannella et al., 2007).

A CIMS is a computer-based software system that facilitates storing, organizing, and analyzing information, managing resources, supporting a common operational picture, maintaining command and

control, and facilitating decision making and collaboration among multiple organizations in order to aid in orchestrating response efforts and sharing of information (Nikolai et al., 2015). They aim to provide a suite of information communication technology (ICT) functions to address the needs of stakeholders involved in the disaster management process. When designing a CIMS, interoperability is a key component of success. Interoperability may be defined as the "ability for two (or more) systems or components to exchange information and to use the information that has been exchanged" (IEEE, 1990). It can also be defined as "a measure of the degree to which diverse systems, organizations, and/or individuals are able to work together to achieve a common goal" (Ide and Pustejovsky, 2010). Interoperability is a key feature provided by CIMS, and it has become essential for disaster management.

To achieve interoperability among disaster response actors, a variety of research avenues have been proposed in the literature. Among these, we identified two sets of related research questions. Our first set of research questions in this paper is:

- Is a given proposed CIMS sufficiently interoperable?

- Does this CIMS meet the challenges of effective disaster response?

We begin by surveying existing CIMSs in terms of their ability to provide interoperability. We found that several points were disregarded by these latter. In each emergency response organization (ERO), there is an organizational structure that defines the responsibilities of different actors in terms of to whom they report and what they do (e.g. allocation of tasks, coordination, and supervision). This organizational structure is defined by the hierarchy forced by its chain of command, something which differs from one ERO to the next. However, these chains of command are neglected by existing CIMSs and the latter therefore do not address the major operational challenges posed by disasters, which call for effective command-response. This shortfall has motivated us to create a new CIMS called POLARISC (Elmhadhbi et al., 2018), which is a semantically driven operational command system based on the French emergency response doctrine that is designed to ensure an effective flow of information among ERs. Our aim is to concentrate on the operational level of disaster response and to address the challenges it faces through software that is designed to provide

reliable and timely information to those involved in the operational management of large-scale disasters. In particular, our focus is on offering to all ERs a real-time operational picture of the situation in order to enable multi-level coordination among firefighters, police, gendarmerie, healthcare services, and public authorities.

Our second set of research questions is:

- How should we design a new common operational command system that satisfies the requirements of all ERs?

- How should we formalize the knowledge of the different stakeholders involved to ensure an effective understanding of the exchanged information among them?

The remainder of this paper is structured as follows: we begin by describing the different levels and stakeholders involved in disaster response and the challenge of coordinating across and among them. We then examine a real use case to illustrate the role of given stakeholders and the value of coordination among them. In section 3, we provide an overview of the main CIMSs, focusing specifically on how they deal with interoperability and with operational challenges. Section 4 details the architecture of the operational command system proposed in POLARISC. Finally, in section 5, the aforementioned use case is used to validate the POLARISC platform.

II. BACKGROUND AND MOTIVATIONS

A. From disaster management to operational disaster response

Disaster management is "the process of planning and taking actions to minimize the social and physical impact of disasters and reduce the community's vulnerability to the consequences of disasters" (Li et al., 2017). It is a multifaceted process that consists of the four main phases of Prevention, Preparation, Response, and Recovery, which are depicted in Figure 1:

1. Prevention means the taking of appropriate strategies to avoid a potential hazard or a natural phenomenon from having harmful event on either people or environment. It is based on hazard identification and vulnerability assessment (evaluation and reduction of risks).

2. Preparation is defined as a state of readiness to respond to a disaster. It consists on taking suitable

measures to ensure efficient rescue planning in terms of stakeholders, funds, and supplies in order to save the maximum number of lives and livelihoods and minimize impacts of anticipated disasters.

3. Response refers to acting in such a way as to respond to disasters as rapidly and effectively as possible by mobilizing the appropriate organizations and resources in a coordinated manner.

4. Recovery refers to the capacity to bring the affected area back to normalcy by assisting the affected community, rebuilding infrastructure, and by providing needed healthcare and rehabilitation (Sena & Michael, 2006).
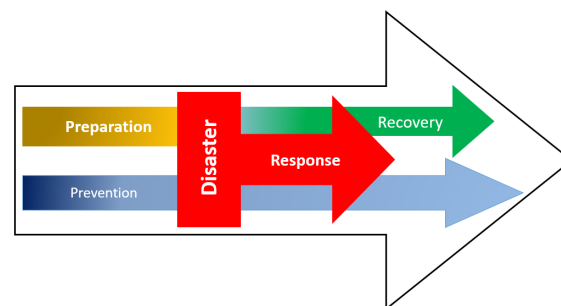

Fig. 1. The disaster management process (International Federation of Red Cross and Red Crescent Societies)

Our focus here is on the response phase of disaster management. When a disaster occurs, a streamlined response resulting from well-coordinated organizations is crucial to its effective handling. This involves knowing what sequence of actions is needed in order to generate a maximally effective response. It also includes decision making within the command team and the communication of its results to the relevant stakeholders together with associated actions such as identifying who the relevant stakeholders are, allocating needed resources, directing search and rescue, evacuating victims, and restoring public order. Planning processes that occur as part of a disaster response process may be conceived as occurring at different levels that correspond to the traditional "levels of war" as shown in Figure 2 ("Three Levels of War", 1997).
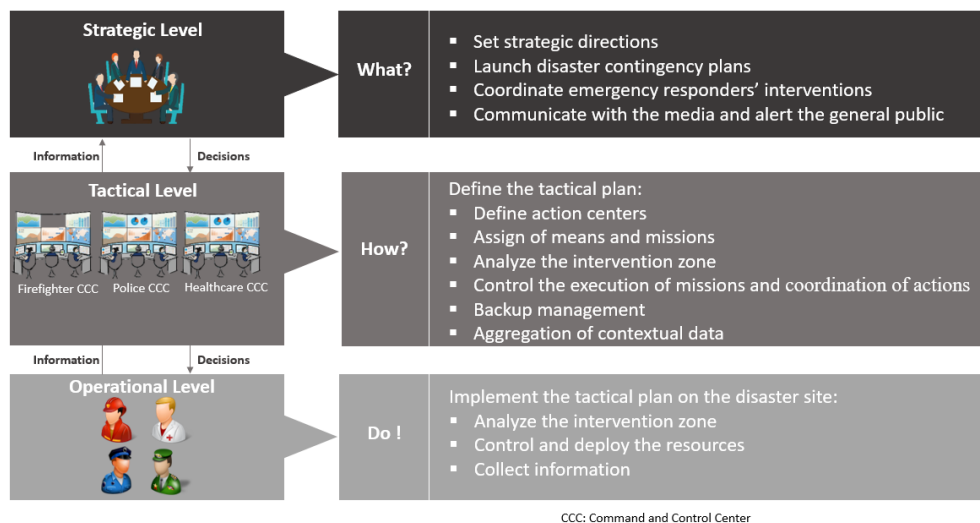
Fig. 2. Levels of disaster response

First is the strategic level. Strategic management is the highest level of decision making handled by public authorities. Which public authority assumes command of the disaster response process is determined on the basis of the type and magnitude of the disaster and of the administrative division of the country in which the disaster occurs. France, for example, is a unitary state in which strategic command depends on four organizational levels. At the national level, the interior minister of France is responsible for civil protection across the whole country. It is he who takes control of the inter-ministerial operational crisis management center, which is tasked with ensuring round-the-clock monitoring of large-scale rescue operations and with coordinating the use of resources in the event of a major incident. At the next level down, zone prefects are in charge of zone operations centers, which ensure the coordination of the rescue operations within their jurisdiction. At the department level, the prefect is in charge of the departmental operations center. The prefect, as the representative of the government of France in each department, relies on the operations command post (PCO), which is located in a safe place near the disaster area and is where the team in charge of coordinating the various stakeholders is located. At the communal level, each commune has its own mayor, responsible for everyday public safety and security on the territory of the municipality. In case of disaster, the mayor is the first to step in. He or she manages resources and coordinates communication among firefighters, police forces, healthcare units, and all actors who may be implicated in the disaster response

process (Coste et al., 2013). The organization of the civil security response plan, known by its French initials ORSEC plan ("Organisation de la Response de Sécurité Civile"), provides the general framework of the response process. This plan directs all inter-services operational response regardless the origin of the major event affecting the population (for example, including both natural and human-made disasters). It defines the chain of command, the responsibility of each actor, the communication protocols. Moreover, it defines the organization and the functioning of the crisis cell which is a joint structure bringing together representatives of the different involved stakeholders. The crisis cell ensures a permanent liaison with the public authority, command and control centers, and actors working on the disaster site. Response efforts need to be coordinated and adapted as the disaster develops through the oversight of a crisis cell.

The role of the strategic level consists of defining strategies and directing the appropriate organizations to engage in responses to a disaster (Brown & Lampen, 2012). It involves, on the one hand, determining high-level directions, including resource priority decisions, assignment of roles and responsibilities, and overall courses of action. On the other hand, public authorities play a key role in disaster communication; they communicate with the media to provide valuable information about events in order to alert citizens and further inter-agency communication. In France, once a disaster occurs, the ORSEC disaster contingency plan is launched. It aims at organizing the civil defense response, under the prefect's authority, through the coordination of the mobilization of all actors. Calling the plan into action means activating five operational cells: fire brigade, medical care, police and public order, transportation, and transmission (Lagadec, 2002).

In practical terms, ORSEC concerns:

1. the establishment of a civil defense network;

2. the definition of an operational doctrine;

3. the implementation through exercises; and

4. the continuous improvement through feedback and lessons learned (Borretti, et al., 2012).

Concerning the tactical level, it means translating strategic objectives into actions. It involves defining the necessary steps for implementing a strategy in order to address a potential threat. There is a separate command

and control structure for each ERO. The tactical level is composed of the commander of each ERO. Their role is to outline what stakeholders must do on the disaster site to successfully respond to the disaster and end threats. It includes also the allocation of resources of each unit on the disaster site according to their availability, task priority, and geographic proximity.

Regarding the operational level, it consists of the major operations conducted in order to accomplish the required tactical plan on the areas of operation. Such operations are intensely monitored since the involved ERs are confronted with uncertainty, time pressure, and highly dynamic situations. They are also highly collaborative processes that require the involvement of different government agencies and multiple emergency responders (ERs) such as firefighters, police, healthcare units, and so on. Ideally, these various ERs should work together and in parallel under a unified command to reach the shared goal of rapid and effective operational response. Derived from the tactical planning, the operational level defines individual tasks to be performed using the available resources. When responding to a disaster, the involved ERs have different roles and responsibilities. For example, firefighters and healthcare services handle the rescue, evacuation and saving lives, police forces and gendarmerie deal with the potential threat and also intervene in the process of evacuation of victims. Usually, the ERs are dispersed at different geographic locations. In other words, some work at the operational command post, and some work in the disaster area. Throughout the operational response collaboration among ERs involves data sharing, which must occur as quickly and efficiently as possible.

In spite of their differences, the strategic, tactical, and operational levels are integrally related. Concerning information flow, the tactical commanders are responsible of information exchange among the strategic and the operational level. Figure 3 presents the disaster response process as a workflow involving healthcare units. It also highlights the interaction that occurs among the different levels and the role of each one.
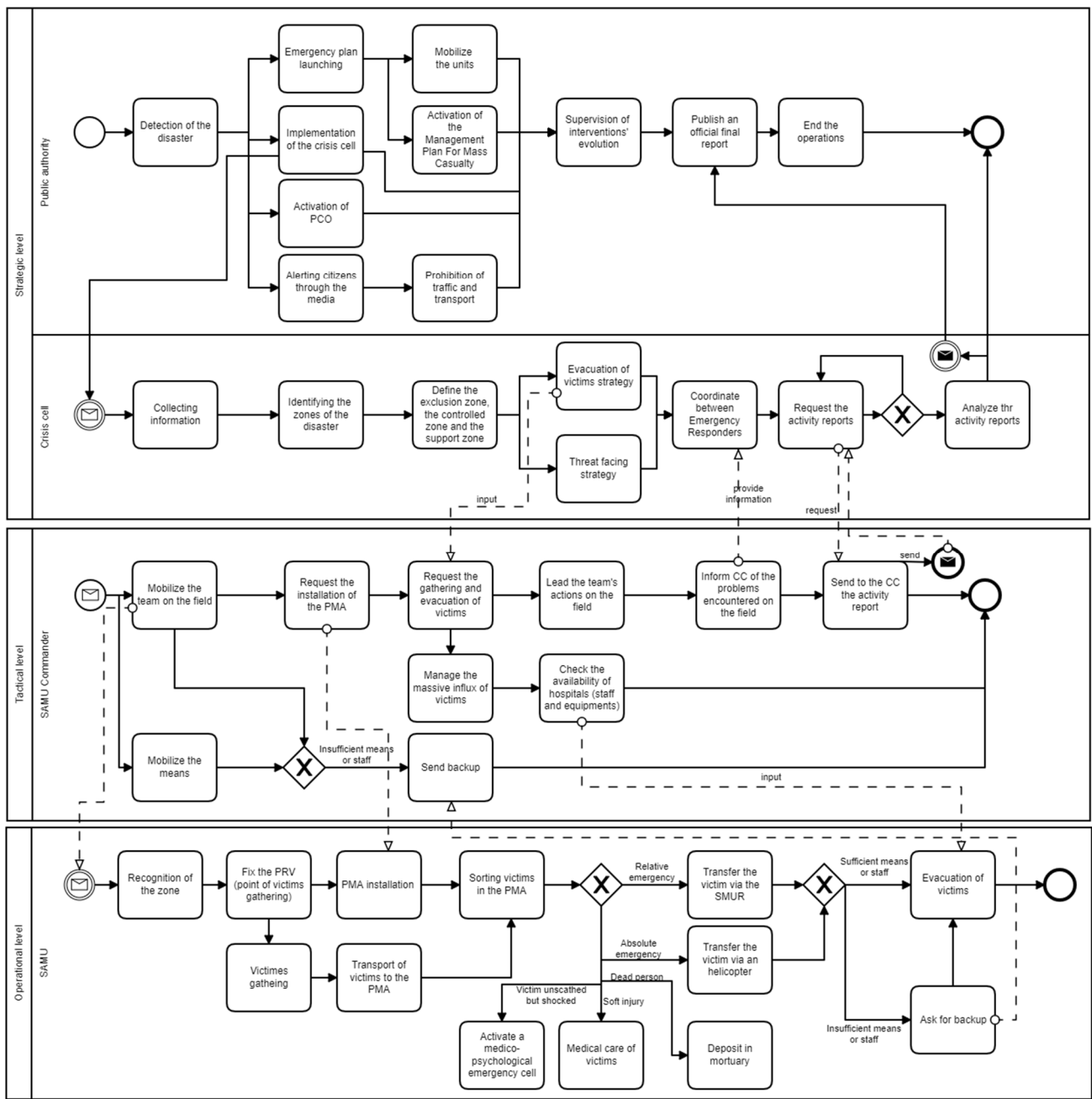
Fig. 3. Example of interaction among healthcare units on the strategic, tactical, and operational levels

B. A motivating case study: 11/13 Paris terrorist attacks

In order to understand how the involved ERs can operate and coordinate their activities when responding to a disaster, here follows an explanation of a real use case. The objective is to analyze stakeholders' interventions and their information processing. We identified the 11/13 Paris terrorist attacks as our case study since it provides several interoperability issues that should be resolved. The data reported here comes

from ER reports. The 11/31 terrorist attacks occurred at multiple sites and were the first of such magnitude in France (Philippe et al., 2016). In all, the attack consisted of six coordinated attacks that were carried out by three groups of gunmen within twenty minutes. At least 130 deaths have been confirmed and 413 were injured and taken care of in Paris region hospitals. The first attack took place at the concert hall "Le Bataclan"; four attackers entered the building and started shooting randomly with automatic weapons. Hundreds of people were held hostage in a theatre. At the same time, during an international football match, three explosions occurred just outside the "Stade de France", a stadium in "Saint-Denis" just outside Paris. Other locations were hit, four bars and restaurants were successively targeted by attackers armed with automatic weapons.

Let us start with the strategic level. Once the terrorist attacks were detected, the interior minister, as the higher public authority responsible for public safety and security on the territory of the region, was the first to step in. First, he launched the emergency plan ORSEC. Second, he ordered the intervention of the elite unit of the national police to make an end to the threats. In addition, the Interior Minister activated the crisis cell. The crisis cell was in charge of collecting the relevant information from the tactical level to identify with precision the attacked zones. As a result, they defined six operational sites. Then, for each site, they ordered the creation of three specific zones (exclusion zone, controlled, and support zone). More specifically, the exclusion zone is an area into which only the police units are allowed to go for reasons of safety. The controlled zone is where the medical team of the police unit transfer the victims to the support zone. This is where we find the healthcare teams and the firefighters. Then, the interior minister activated the command post of each operational site in order to coordinate actions of the various ERs on the disaster site. Moreover, the health emergency contingency plans (the Plan Blanc and the Plan NOVI for mass causality incident) were activated by the director of the centralized Parisian hospital's authority crisis management center (APHP). To do this, the APHP managing director sent a message to alert all hospitals in Paris, alerting them that the activation of the Plan Blanc is imminent. In fact, the role of the APHP was to coordinate medical rescue efforts of the forty hospitals in Paris and orienting patient care according to the needs and resources

availability (for example, bed management) (Ghanchi, 2016). The APHP managing director also kept other hospitals ready as a backup, in case the hospitals launched into action by the Plan Blanc weren't sufficient.

At the tactical level, the leadership of every ERO was in charge of mobilizing their unit and allocating the appropriate means on the disaster site. During the response, the command and control of the involved stakeholders were carried out by the commander of rescue operations (e.g. firefighters), director of the medical response (e.g. healthcare units) and the commander of police operations (e.g. police forces). This meant they were responsible for sharing information with those at the strategic level by informing the crisis cell about what was happening on the sites, as well as directing ERs' actions, and managing resources.

At the operational level, the ERs responded to these terrorist attacks in extremely volatile and difficult circumstances. Each stakeholder had a specific role to accomplish on the disaster site under a unified command center. In particular, the elite unit of the police force focused on finding, apprehending, or neutralizing the assailants on one hand, and releasing the concert hall's hostages on the other hand. Another team of the police forces defined the security perimeter by dividing it into exclusion, controlled and support zone. Then, they started the extraction of victims to the controlled zone in order to evacuate the affected area and transport people at risk to safety. There were victims in an absolute emergency and it was not possible to move them. Therefore, the police and healthcare units, known by its French initials SAMU, have developed a method to support healthcare staff entering scenes where terrorist attacks have occurred to provide immediate care to these victims, as well as helping to move victims to safe areas. Simultaneously, the gendarmerie teams secured and isolated the defined zones by prohibiting the access of the public or the media in order to facilitate the arrival of ERs.

Once the victims were transferred to the support zone, the healthcare units installed the advanced medical post (known by its French initials PMA). Then, firefighters collaborated with healthcare units in the gathering, rescuing, and evacuating processes. They transferred the victims from the point of victims' gathering (PRV) to the PMA to do the triage of the injured victims in order to determine the priority of victims' treatments based on the severity of their condition and then to perform the evacuation. Victims who

were in a relative urgency were transferred to the activated hospitals. Those who were in an absolute urgency were transferred immediately via a helicopter. Concerning victims with soft injury, they received instant medical care. Finally, victims that were unscathed but in shock were being taken care of in the medico-psychological emergency cell.

Because the ERs were organized using a hierarchical command and control system, one might infer that the orders issue from the strategic level to the tactical level at first and then to the operational level. In fact, there was no direct communication among ERs from different EROs (Emergency Responders Organizations) on the disaster site and also among operational ERs and the strategic level. Instead, each actor informs the unified command center of the situation as it evolves via their representative. For instance, once the police forces neutralized the terrorists and secured the concert hall, they removed the exclusion zone so that the healthcare units could continue to evacuate the rest of the victims. To do so, the steps of information flow is like follow (Figure 4). the operational commander of the police forces informed the tactical commander: (1) who reported it to the crisis cell (2). This latter informed the public authority (3). Then, the public authority ordered the intervention of the healthcare units (4) then the crisis cell informed the healthcare commander about the decision (5). This latter defined the evacuation plan and required its execution on the disaster site (6). After studying the use case, one may notice that coordination and information flow among stakeholders on the scene is key to an effective disaster response.
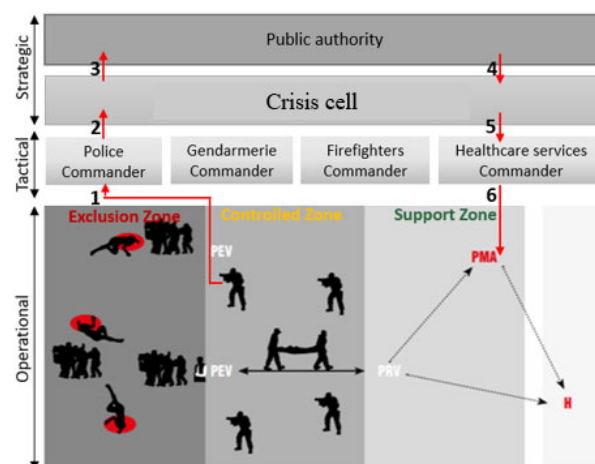

Fig. 4. Example of information flow among emergency responders during an operation

C. Operational disaster response: Challenges to effectiveness

ERs are still facing a lot of challenges when responding to a disaster. Numerous after-action reports from major disasters have cited communication difficulties among EROs as a major challenge (Clarke, 2003) and expressed concerns over the EROs' ability to collaborate. An example of this can be found in the concluding report on the terror attack in Norway on June 22, 2011, stating that the various EROs (including firefighters, police, healthcare services, and others.) were unable to effectively communicate and coordinate their effort. Furthermore, these challenges were highlighted by the 9/11 and 11/13 terrorist attacks where ERs shared information that created a disorganized multi-agency response (Kean and Hamilton, 2004). Almost fourteen years pass between the two terrorist attacks and the challenges remained the same. In the 11/13 Paris attacks, police forces claimed that (Nossiter, 2015):

- "by the time the information gets out and reaches up, mobilizing the specialized units takes a relatively long time."
- "our police are not organized along local lines. Everything has to filter up to the central organization at the prefecture."
- "We have a police force that is disconnected from the field."

Furthermore, on the night of the terrorist attacks, there were two sites, where victims did not receive medical care due to a lack of communication between firefighters and healthcare units (Philippe et al., 2016).

The need for all actors to be able to communicate when responding to a disaster or treating victims is vital. Respectively, the importance of communication during a disaster for collaboration is indisputable (Kristiansen et al., 2019). But, each ERs has deployed its own information system adapted to its own needs, resources, and processes. As a result, the communicated information is heterogeneous as each communication is stored and transferred in different data sources, with different formats and semantics. Semantic heterogeneity of data and the absence of a common language are becoming ever more important issues as the amount of data is growing (Kristiansen et al., 2019). These issues lead to misunderstanding and a lack of data sharing among the ERs that can handicap the response process and slow decision making (Bharosa et al., 2010).

Moreover, the use of radio communication by each actor makes inter-organization communication extremely difficult (Manoj & Baker, 2007). All too often, the operational actors find themselves during the intervention with poor radio coverage. In a recent survey of EROs (in Building Public Safety Communication Survey, 2018), more than 65% of ERs said they had experienced some sort of communication failure within the past twenty-four months while responding to an emergency. Moreover, in the Paris attacks, firefighters and healthcare units pointed out that the use of radio communication means such as ANTARES network has not been satisfying during the different interventions (Boutinaud, 2017). An additional problem is that radio communication does not enable information tractability and consolidation. The availability of a technical communication infrastructure has been shown to be a strong predictor of success or failure during disaster response operations (Steigenberger, 2016).

Furthermore, after Hurricane Katrina in 2005, the ERs highlighted the need to have a comprehensive operating picture in order to improve understanding and facilitating decision making to provide situational awareness. There is a need to provide a common understanding of what situational information is needed, how that information is displayed, how it is achieved and how it is updated throughout the life of the intervention (Smith, 2012). To be comprehensive, an operating picture must consider the terminology and the graphical charter of each ER. In addition, another important difficulty during disaster response is to find the best allocation of available resources so as to reduce casualties. ERs work together to ensure that those causalities are gathered and transported to an appropriate hospital in a minimum of time. But this process can be more complex if it concerns a multi-site response with limited resources. That is to say, the allocation of resources is a big challenge for ERs during the operational response.

To summarize, it becomes clear that there are various factors that influence operational disaster response. Figure 5 recapitulates the various challenges that should be considered for an effective multi-agency disaster response. These challenges are the keystone of the efficiency of disaster response. They are related to communication, collaboration, information, and resource allocation. As a result, recognizing the need for enabling interoperability among ERs systems is crucial. In fact, interoperability is considered as the key

component that empowers data sharing and the orchestration of the collaborative process in order to build a coherent response to the crisis. It enables ERs to have access to the right information, in the right format, at the right time; this solves those issues that limit collaboration among the involved stakeholders during multi-agency responses (Salmon et al., 2011).
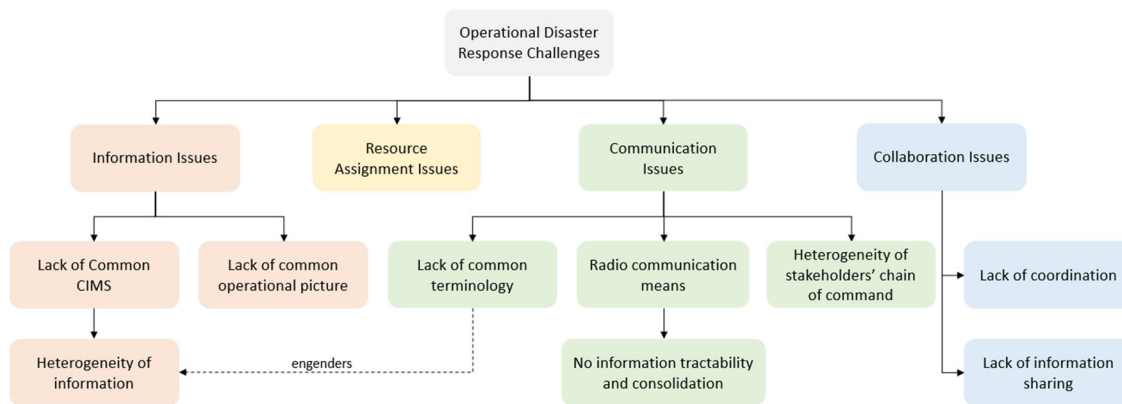

Fig. 5. Challenges to operational disaster response

III. STATE OF THE ART: POSITIONING IN ENTERPRISE INTEROPERABILITY FRAMEWORK

In the literature, a variety of CIMSs have been proposed. They focus on one or more aspects of the aforementioned challenges of the operational disaster response that need to be resolved to ensure information sharing and reliable communication for coordinated interventions (Li et al., 2017). In what follows, we investigate how interoperable these systems are by looking at some existing projects.

A. The Framework of Enterprise Interoperability

The Framework of Enterprise Interoperability (FEI) was introduced by the European Virtual Laboratory for Enterprise Interoperability (I-VLab) and is now published as an international standard (ISO 11354 - 1) (Chen et al., 2007). It defines a classification scheme for interoperability knowledge according to three major dimensions. First, interoperability can be characterized by concerns. Second, solutions to interoperability problems can be characterized according to interoperability approaches. Third, interoperability problems can be localized into interoperability barriers. There are three types of barriers: First, conceptual barriers concern syntactic and semantic differences of information to be exchanged. In this context, syntactic incompatibility

of information means that there are different formats to represent information that prevent them from being combined and accessed, and then the semantic incompatibility of information means that there is no defined semantics that enables unambiguous understanding of the information. In disaster response, each ER requests information in their own vocabulary, data representation, and graphical charter while information is stored in different data sources, with different semantics, and in different formats. In other words, it is necessary to develop a common semantic terminology to coordinate ERs. Second, technological barriers concern the absence of compatible standards that enable the use of heterogeneous ICT for sharing and exchanging information such as incompatibility of middleware platforms, protocols, and so on. These barriers point to the absence of middleware among the heterogeneous information system used by ERs. Since each stakeholder has deployed his own information system using specific technologies and standards, these latter cannot be interoperable. Third, organizational barriers are related to the incompatibilities of organization structure (authority and decision-maker) and their responsibility.

 Interoperability concerns are four: Data, Service, Process, and Business. First, data interoperability refers to the capability of easily finding, sharing, and understanding data from heterogeneous databases on different machines with different operating systems. Second, the interoperability of service refers to the ability of various independent applications to work simultaneously. Third, the interoperability of process aims to make several processes work together, where a process may be conceived as a sequence of performed services. Finally, interoperability of business refers to a harmonized way of working across organizations. The interaction among these concerns according to ERs are like the following; data (different semantics, in different formats and stored in different databases of ERs) is employed by services (different functions and roles of each stakeholder) and services are used by process (coordination of ERs' processes of intervention) to perform business (multi-organization response to a disaster).

   Concerning interoperability approaches, it enables interoperability among systems is not only a matter of removing barriers; it also matters how these barriers are removed (Chen et al. , 2007). There are three ways in which barriers can be removed: First, the integrated approach refers to the use of a common format

(standard) for all models. It concerns the integration of systems more than interoperability of systems. The main objective of this approach is to guarantee the global stability and coherence of the different systems. Secondly, the unified approach signifies that there is a common format only at a meta-level. It establishes semantic equivalence among information in order to enable the mapping among models. But this may engender the loss of some semantics. Finally, the federated approach holds that there is no imposed format at all but, instead, there is a shared ontology.

To sum up, each intersection among a concern, a barrier, and an approach is an interoperability research area. The different CIMs proposed in the literature may be positioned into the FEI to highlight the studied interoperability barriers and concerns, and the corresponding approaches to point out the neglected points that should be considered.

B. Study of Crisis Information Management Systems

In the following, we analyze several recent projects. In (Cinque et al., 2015), the authors proposed a CIMS as part of the project SECTOR (Secure common information space for the interoperability of first responders). Authors proposed a common information space (CIS) that provides users "peer-to-peer" functionalities to dynamically establish cross-agencies and cross-borders collaborative platform. That is to say, by means of the proposed CIS, the authors established a unified approach to enable interoperability among multi-organizations systems by removing conceptual and technological barriers. From an operational point of view, this work focused only on decision making within disaster response organizations in order to optimize the process of resource allocation.

Let us focus now on the European project DISASTER (Data Interoperability Solutions at STakeholders Emergencies Reaction) that seeks to solve the task of information sharing and coordination among international workforces (Casado, 2015). The authors proposed a software application that mediates communication among different CIMS. To support the mediation and to provide organizations with the needed information, DISASTER is based on a common modular ontology named EMERGEL that considers the linguistic, semantic, and cultural differences among countries. So, the authors followed a federated

interoperability approach and proposed an ontology that will be used in translating emergency-related terms in cross-border disaster response. They tried to remove conceptual and technological barriers to ensure interoperability among data and services. Furthermore, the DISASTER project focuses mostly on the strategic level of disaster response in cross-border situations. The DISASTER project underrepresents information sharing and collaboration among operational ERs on the disaster site. Moreover, the semantic mapping of information is left out and end-user requirements were not identified.

In (Cinque et al., 2016), the authors propose a CIMS named DESTRIERO (A DEcision Support Tool for Reconstruction and recovery and for the IntEroperability of international Relief units in case of complex crises situations, including CBRN contamination risks). It is a middleware platform for messaging, knowledge management, and data transformation in large-scale disasters (Cinque et al., 2015). DESTRIERO pursues a federated interoperability approach by proposing a standard-based formal ontology in order to remove conceptual and technological interoperability barriers by resolving technological, syntactical and semantic heterogeneity of data occurring among organizations. From an operational point of view, the proposed CIMS architecture provided a tool for data exchange among actors at the tactical level of disaster response, and it fails to represent the graphical charter that signate ERs' vocabularies to represent what is happening exactly on the disaster site. Moreover, there is no real prototype of the proposed architecture.

In the European project SecInCoRe (Secure Dynamic Cloud for Information, Communication and Resource Interoperability based on Pan-European Disaster Inventory), the authors conducted a Pan-European inventory of disasters and their consequences. They then elaborated a dynamic cloud-based communication system concept. The authors proposed a federated interoperability approach by proposing a shared ontology created by reusing vocabularies, glossaries, and semantic approaches, although the proposed CIS focused on enabling interoperability only among first responders and police forces.

The SoKNOS project proposes a prototype of an ontology-based CIMS for creating a mutual understanding between developers and end-users across different organizations (Babitski et al., 2011). In fact, information sources and services are annotated with ontologies in order to connect existing systems and databases to the

SoKNOS system. Thus, SoKNOS focuses on ensuring conceptual interoperability of data by proposing a federated approach by using an ontology to formalize the knowledge of the heterogeneous organization involved in the process of disaster management. However, they did not consider all the involved ERs (only firefighters and police forces) and their technical vocabulary.

DRIVER project (Driving Innovation in Crisis Management for European Resilience) proposes a distributed Pan-European test-bed to provide guidelines on how to perform experiments as well as a framework to evaluate the results (Havlik et al., 2016). It suggests communication solutions among disaster response managers and citizens (or unaffiliated volunteers). DRIVER is also related to other projects, such as DARWIN2, which aims to provide emergency responders guidelines so as to facilitate disaster response. To summarize, DRIVER and DARWIN2 both propose integrated interoperability approaches to remove technological barriers of data and services among stakeholders and volunteers. However, the experiments of these projects have clearly demonstrated technological shortcomings that need to be addressed. Moreover, they do not resolve the deficiency of communication and coordination among operational stakeholders and these challenges are the key to a successful disaster response.

IsyCri (Bénaben et al., 2016) is a French project that provides an information system in order to enable interoperability among the actors responsible for the reduction of disaster situations. To accomplish this task, their strategy is to merge the information systems of the different involved stakeholders into a global system. The authors tried to remove technological and organizational barriers by proposing a unified interoperability approach. The IsyCri project focuses more on meta-ontologies to structure and formalize concepts related to disaster response. This information system targets the orchestration of the collaborative process of the strategic level of disaster response and does not resolve the challenges of inter-services operational response.

The RESCUER project (Reliable and Smart Crowdsourcing Solution for Emergency and Crisis Management) proposes a smart interoperable CIMS that supports a disaster response command center (Villela et al., 2014). It gathers, creates data visualizations, and manipulates information provided by the people present at the place of the incident. This system is addressed to the strategic level of disaster response

in order to collect relevant missing contextual information about the disaster from eyewitnesses and then communicate instructions to the affected people, ERs, public authorities, and also the press. To do so, the authors propose a federated approach, an ontology-based data-exchange solution to allow semantic interoperability between RESCUER and the command center (Barros et al., 2015). The ontology is defined on the basis of the Emergency Data Exchange Language (EDXL). However, RESCUER does not cover information exchange among ERs on the disaster site.

In (Vidan and Hogan, 2010), the authors have been working on a prototype command and control system, LDDRS (Lincoln Distributed Disaster Response System), that enables shared situational awareness and collaboration during response operations. They propose an integrated interoperability approach to display a map of an area of interest, on which is located staff and vehicles. They propose a real-time common operational picture accessible by all ERs but it doesn't consider the details of what is happening on the scene. It shows only the position location information of vehicles and staff.

Table 1 and Table 2 summarize the comparisons of CIMSs proposed by the previous highlighted projects in terms of interoperability approaches, concerns, and barriers, and operational challenges.

This review makes clear that there is still a great need to improve CIMSs for disaster response. There are interoperability concerns (process and business) and barriers (organizational) that are neglected despite their major importance and their impacts on disaster response. On the one hand, organizational barriers were disregard by the studied CIMSs because the focus of these latter is mainly on the strategic level of disaster response. Indeed, organizational barriers should be considered in operational disaster response, given that the hierarchical chain of command and the nature of the involved actors vary from one organization to another. Each stakeholder fulfilling a role has a clear route of communication up and down the chain of command. That is, a good understanding of the hierarchical chain of command of each ERO can greatly impact information flow and decision making. The consideration of organizational barriers will eliminate the confusion caused by several and conflicting commands. On the other hand, process and business are two major concerns that should be considered when addressing interoperability requirements. Together, they

represent the orchestration of stakeholders' actions within different organizations and their collaborations in a coordinated and harmonized manner.

There is no system that resolves all the challenges of disaster operational response. Various CIMS have proposed the use of a federated approach to overcome semantic heterogeneity of data among stakeholders. We believe that the use of ontologies and the development of a common terminology is essential to guarantee a consistent shared understanding of the meaning of information to be exchanged.

Overcoming the aforementioned problems motivated us to propose POLARISC, an ontology-based CIMS that concentrates on the operational level of disaster response by considering all the cited challenges. It ensures interoperable communication and information sharing across all ERs involved in the process of disaster response, preserves a suitable coordination of their actions, guarantees an appropriate visualization of what is happening exactly on the disaster site by taking into consideration the technical vocabulary and graphical charter of each ERs. In terms of interoperability, POLARISC proposes a federated and integrated approach to resolve conceptual, technological, and organizational barriers concerning data, service, process, and business.

In the literature, the Incident Command System (ICS) and the Multiagency Coordination System (MACS) have been developed as the official management tools adopted by EROs in the united states to respond to all types of incidents from day-to-day emergency to large-scale disasters. Mainly, the ICS has five major functions: command, planning, operations, logistics, and finance/administration. According to (Jensen & Thompson, 2016) (Lindell et al., 2005), ICS necessitates further improvements to enable adequate coordination between the Incident Command Post and other activities away from the incident scene. To tackle this problem, POLARISC will effectively enhance coordination during large-scale disaster response by enabling unambiguous information exchange and real-time operational picture of what is happening on-scene. The aim is to provide stakeholders, that are away from the disaster scene, with the right information at the right time to support decision making. POLARISC adopts the ICS best practices to successfully facilitate command and control, communication, coordination, and decision making.

Table 1. Comparative study of CIMS basing on the Framework of Enterprise Interoperability

Projects	Approaches			Barriers			Concerns				Literature
	Integrated	Unified	Federated	Conceptual	Technological	Organizational	Data	Service	Process	Business	
SECTOR	×	✓	×	✓	×	×	✓	✓	×	×	(Cinque et al., 2015)
DISASTER	×	×	✓	✓	✓	×	✓	✓	×	×	(Casado, 2015)
DESTRIERO	×	×	✓	✓	✓	×	✓	×	×	×	(Cinque et al., 2016)
SecInCore	×	×	✓	✓	✓	×	✓	×	×	×	(Schäfer et al., 2017)
DRIVER	✓	×	×	×	✓	×	✓	✓	×	×	(Havlik et al., 2016).
DARWIN	✓	×	×	×	✓	×	✓	✓	×	×	(Havlik et al., 2016)
ISYCRI	×	✓	×	×	✓	✓	✓	✓	✓	✓	(Bénaben et al., 2016)
SOKNOS	×	×	✓	✓	×	×	✓	✓	×	×	(Babitski et al., 2011)
RESCUER	×	×	✓	✓	×	×	✓	×	×	×	(Villela et al., 2014)
LDDRS	✓	×	×	×	✓	×	✓	✓	×	×	(Vidan and Hogan, 2010)

Table 2. Comparative study of CIMS basing on the operational response challenges

Projects	Communication	Information sharing	Common terminology	Common CIMS	Real-time operational picture	Resources allocation	Literature
SECTOR	×	✓	×	×	×	✓	(Cinque et al., 2015)
DISASTER	✓	×	✓	✓	✓	×	(Casado, 2015)
DESTRIERO	✓	×	✓	×	×	×	(Cinque et al., 2016)
SecInCore	✓	✓	✓	×	×	×	(Schäfer et al., 2017)
DRIVER	×	×	×	×	×	×	(Havlik et al., 2016)
DARWIN	×	×	×	×	×	×	(Havlik et al., 2016)
ISYCRI	×	×	×	✓	×	×	(Bénaben et al., 2016)
SOKNOS	×	×	✓	×	×	×	(Babitski et al., 2011)
RESCUER	×	×	✓	×	×	×	(Villela et al., 2014)
LDDRS	×	✓	×	✓	✓	×	(Vidan and Hogan, 2010)

IV. PROPOSED SOLUTION: POLARISC

The aim of POLARISC is to concentrate on the operational level of disaster response and to consider the cited challenges by proposing a semantics-based interoperable operational command system. The aim is to ensure reliable and timely information sharing among stakeholders involved in the process of disaster response. Figure 6 illustrates the architecture of POLARISC platform as a whole system. POLARISC is addressed to all ERs including firefighters, police, gendarmerie, healthcare units, and public authorities to enable coordination during the multi-agency response. It is a software solution that plays the role of mediation among ERs. It is composed of three layers; user interfaces layer, mediation layer, and the core layer.

First, concerning the users' interface layer, POLARISC aims to offer a real-time operational picture of what is happening on the disaster site by considering the different graphical symbols and colors' codes of each stakeholder. It is built based on the French national graphical charter of ERs. Using the proposed platform, each stakeholder can place units, action centers, and resources on the map to represent the situation on the site according to the topology of the field, the weather, the direction and strength of the wind. In order to achieve it, an icon repository is deployed. The operational picture is generated by the geospatial resources data. The latter are composed of data about geographic location represented primarily by images and tables or grids of observed or calculated attributes. These resources are used in our system for purposes of cartographic mapping to enable the visualization of the common operational picture of the disaster site. Second, the POLARISC mediator is responsible for guaranteeing an appropriate understanding of the situation by the different ERs. It plays the role of gateway between end-user and the core system so as to provide a suitable representation of the requested data according to stakeholder's characteristics (for instance, their vocabularies, the graphical symbols that signate them, the color codes assigned to them.). Accordingly, all information exchange is organized and distributed to all involved ERs by POLARISC mediator. The aim is that ERs will be able to understand external information and all parties share the same extent of such derived information. Third, the core system is composed of a knowledge base, a set of integrated services

and geospatial resources bases. The map server and the knowledge base server generate real-time data that will be used as input in the services component.
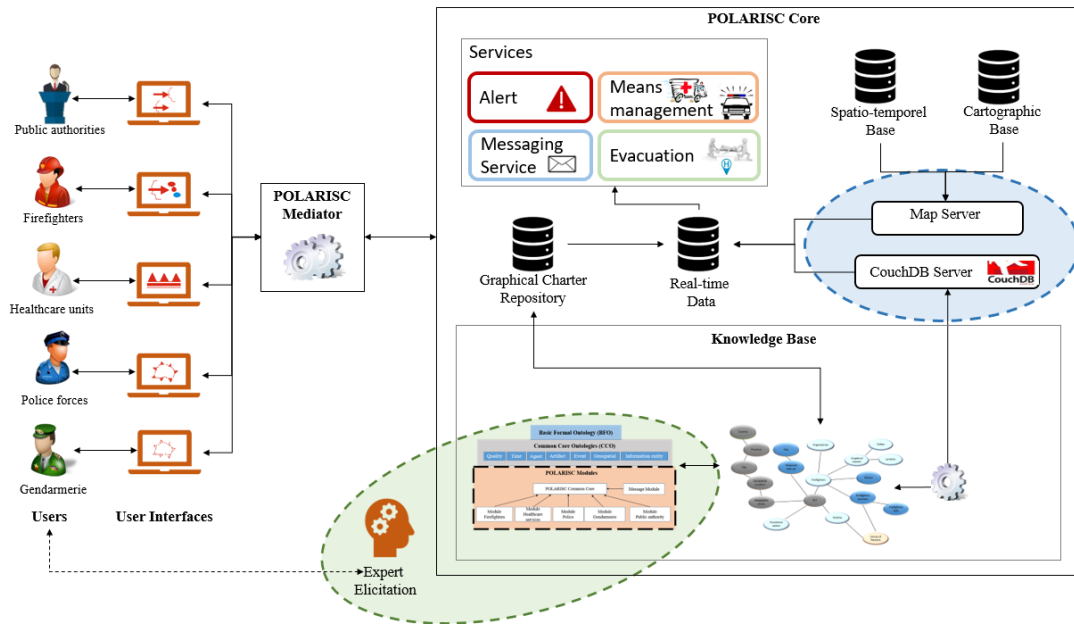

Fig. 6. POLARISC architecture

A. POLARISC ONTOLOGY

(Gruber, 1995) defines an ontology as "an explicit and formal specification of a shared conceptualization". Ontologies are expressed in a formal, machine-readable language, so that meaningful distinctions can be made among the classes, instances, properties, attributes, and relations. The ontology serves as both knowledge representation and as mediation to enable heterogeneous systems interoperability (Song et al., 2013). To overcome semantic heterogeneity among stakeholders, the definition of a common terminology is essential. Thus, we turn to ontology to reveal the ERs' complex knowledge in order to understand the meaning of the exchanged data by ERs. Accordingly, we propose a knowledge base composed of a modular suite of ontologies named POLARISCO. Ontology, together with a set of instances of its classes constitutes a knowledge base that includes: concepts, properties, and the relationships among them, and rules (Dang et al., 2008). It is the main source of information, capable of being exploited by all the stakeholders. Such a shared vocabulary resolves terminological inconsistencies and establishes semantic interoperability among

ERs. It formalizes the complex knowledge of the French ERs. Moreover, it represents all the key kinds of processes associated with disaster response and all levels (strategic, tactical and operational) and it defines the technical vocabulary of all the involved stakeholders (e.g. means, roles, action centers, processes). In particular, POLARISCO takes into account four perspectives:

- *What:* POLARISCO defines the different kinds of disasters (disaster's type, needed resources, the corresponding acts, etc.).
- *Why:* Each ER has its own process of intervention, means, roles, and so on. This may have consequences for the collaboration among the involved actors.
- *Who:* POLARISCO defines the vocabulary of each actor including firefighters, police, gendarmerie, healthcare units, and public authorities. Furthermore, disaster response includes taking care of victims. Accordingly, we define victims and their different states.
- *Where and when:* A disaster occurs in a specific spatial-temporal region. These latter are fundamental to effectively respond to a disaster. For this purpose, POLARISCO provides a temporal and geospatial description of disasters and stakeholders' actions.

Considering the diversity of ERs' vocabularies, we adopted the principles of modularization to build our ontology (a module for each stakeholder). Modularization is considered as a strategic way of structuring sets of related ontologies. Thus, the construction of a large ontology is based on the combination of self-contained, independent, and reusable modules (D'Aquin et al., 2007). The main advantages of such a method include the ability to manipulate smaller ontologies, the reduction of the complexity of ontologies development, and reusing each module independently. First, a module is defined for each stakeholder. We propose five modules to encapsulate the knowledge of the different involved ERs, namely firefighters module, healthcare units module, police forces module, gendarmerie module, and public authorities module. Then, we define a message module to represent the needed knowledge to formalize information exchange among ERs and to improve communication capabilities. As a matter of fact, we found that there are several terms in common among the stakeholders defined modules, which led us to define a core module named POLARISC Common Core (PCC). It includes the general classes that all stakeholders share (for example, types of disasters, spatial and temporal regions of disasters, transmission means, victims) in order to ensure more semantic interoperability among the modules and to facilitate their integration. To aid ERs in overcoming the problem

of data heterogeneity, POLARISCO is an extension of BFO (Basic Formal Ontology) and CCO (Common Core Ontologies) that integrate eight modules:

- POLARISC Common Core (PCC) module
- Firefighters module
- Healthcare units module
- Police module
- Gendarmerie module
- Public authorities module
- Messages module
- Healthcare resources module

In (Elmhadhbi et al., 2019), the ontological approach of the development process of POLARISCO is presented in detail. Concerning the stakeholders modules, we used the PCC module as a starting point, and then we added the appropriate classes related to each module. For each stakeholder module, we defined services and members for each EROs, the role of each member and their type (command or operational), their specific acts, the used means, action centers, and so forth. Furthermore, we used the relation *"supervises"* defined by CCO among the different roles to put forward the hierarchic levels of command. Once the modules were developed, we defined the mapping between these latter to establish the equivalent classes and relationships that will be the key to ensuring the precision and the relevance of the exchanged information during the semantic translation processes among different ERs. These manual alignments are validated by ERs experts. Figure 7 shows a partial view of the stakeholders modules.
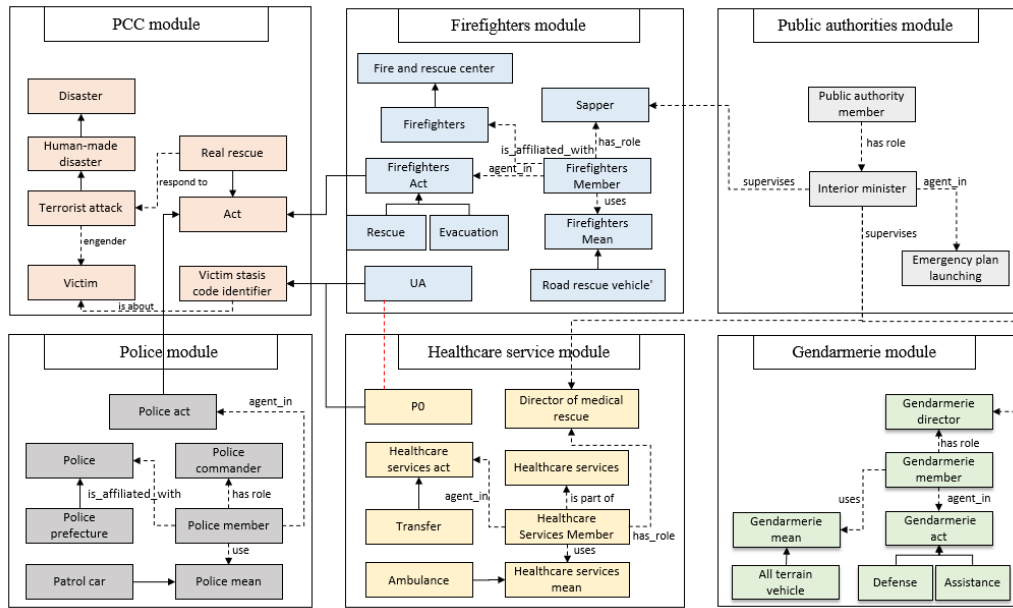
Fig. 7. Partial view of stakeholders modules

For example, the public authorities module is linked to the rest of the stakeholders modules with the relationship "supervises". That is to say, the interior minister supervises the commander of each ER. In fact, annotations and equivalent classes will have a key role later in the messaging service. Specifically, they will enhance communication capabilities and enable the semantic transformation of the exchanged information from one stakeholder to another. Accordingly, each stakeholder will receive information according to their own vocabulary. The message module is related to the PCC module and subsequently to the stakeholders 'modules. To define it, we reused classes from the PS/EM Communication Ontology (Chan et al., 2017). The authors based it on the EDXL-RM (Emergency Data Exchange Language-Resource Messaging) standards.

Moreover, the ontology contains references to symbols in the graphical charter repository (Figure 8). The latter contains all the symbols used by firefighters, healthcare units, and police forces. These symbols are tactical symbols that represent the limit of the action center, the kind of the mean used, the number and the type of the engaged units on the site, the type of the action, a color that represents the type of the threat (e.g. red for fire, blue for water). The mapping among these symbols is the keystone of ensuring an understandable operational picture to each stakeholder.
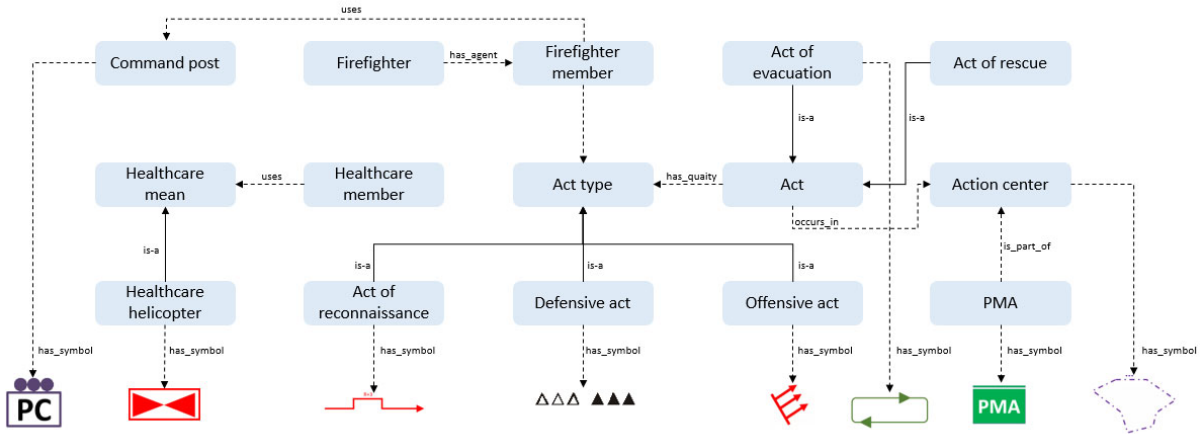
Fig. 8. Common operational picture of the disaster site

To query and infer new knowledge from the ontology, the semantic query language SPARQL is employed. To use the ontology, POLARISCO is serialized in both OWL and JSON-LD and stored in CouchDB. This transformation is accomplished using Protégé. CouchDB is an open-source NoSQL database. It is also a document-oriented database that can be requested by HTTP. Our adoption of it is driven by the fact that CouchDB enables the application to be used offline. The real-time common operational picture of the disaster site and information exchanged among ERs is based on the internet connection, which is unreliable. That is to say, thanks to CouchDB, all the features of POLARISC platform can be used offline to store data and to make it available once the system is back online.

B. *POLARISC SERVICES*

POLARISC is intended to enable a set of integrated services designed to support the ERs when responding to disasters. Among these services, the evacuation of victims facilitates the process of taking care of victims by finding as quickly as possible the appropriate healthcare institutions and reserving it according to the patient state (Mhadhb et al., 2015). The alert service aims to improve ways stakeholders respond to disasters by delivering emergency alerts and warnings to the public. It also aids other ERs not far from the disaster site in preparing to send backup if it is needed. The means management service will facilitate the process of assigning resources to the disaster site by checking its availability. Finally, the messaging service PROMES

(for POLARISC Ontology-Based operational MEssaging Service) is responsible for ensuring semantically enhanced information exchange among ERs. Such a service demonstrates the potential of using POLARISCO in order to resolve terminology inconsistencies for supporting communication and ensuring mutual understanding among the involved stakeholders. The main purpose of the messaging service is that each stakeholder will receive information according to its own vocabulary and with its own semantics. The semantic translation of the information to be exchanged is based on the semantic relationships defined among stakeholders ontological modules. This service is used on-demand by POLARISC mediator to perform the semantic translation of the information to be exchanged.

There are various types of messages to be exchanged among ERs at the operational level as defined in POLARISCO. Each ERO has a predefined structure that may be used to compose each type of message to guarantee the clarity of the information to be exchanged. Accordingly, we developed a graphical user interface that respects the predefined structures so that each stakeholder inputs the needed information using its own vocabulary with respect to POLARISCO (Figure 9). Once the type of message is chosen, the user is directed to select the appropriate classes from the proposed lists. The next step is the structural transformation of the message from a set of classes to a textual message based on the pre-defined structure of the exchanged information of each ERO in order to ensure the understanding of the message. Then, PROMES semantically translates the message; it transforms data expressed according to the ontological module of the sender into equivalent data in different domain knowledge defined using the ontological module of the receiver. For this reason, we employ an algorithm (it is out of the scope of this paper) that, for each class of the set, searches the correspondences between the ontological module of the sender and the ontological module of the receiver. We consider three possible kinds of mapping among classes. The most frequent relationship among entities is equivalence, which allows us to substitute a class for its equivalent class. However, in case there is no equivalent class found, we add more information about the class using the class' annotations (e.g. definition and acronyms). If this still fails, we substitute the class with its superclass.

Fig. 9. PROMES' guided user interface

These different services enable information consolidation and tractability that, on one hand, facilitate the decision-making process, on the other hand, support the learning process in order to ameliorate disaster response strategies. Specifically, once the response process is over, POLARISC generates an activity report that resumes the on-scene operations and recapitulates the engaged resources, actions, action centers, commanders, etc. The strategic commanders rely on this activity report as feedback to continuously improve the strategies of resource allocations and so on.

V. POLARISC: USE CASE

To validate and verify the developed elements, we discussed the 11/13 Paris terrorist attacks, presented in section 2.1. As a first step, stakeholders must log into the application to use the platform. Once logged in, they should create a new intervention by specifying where and when the disaster occurred. Once the intervention is created, a new map is available. Given this new map, ERs are able to represent the operational activities on the map to establish a real-time operational picture. We use ERs feedback to represent the

operational picture of the action center of the firefighters as shown in Figure 10. Symbols are placed on the map such as units, vehicles, PMA, actions, and action centers. Whenever new information is added, it is updated on the platform. Using POLARISC mediator, the rest of the stakeholders can visualize the same operational picture but using their own graphical symbols. This real-time visualization is accessible to all the levels of disaster response. POLARISC end-user platform is used by the unified command center, the different command and control centers, the command post of each ERO, and stakeholders on the disaster site. Figure 11 depicts a comparison between the firefighters' command post using whiteboards when responding to a disaster and then using POLARISC platform. One can notice that real-time exchanges take less time than usual and increase response efficiency and effectiveness.

Fig. 10. Common operational picture of the disaster site

Fig.11. The use of POLARISCO in the Command Post

Afterward, to test the usability of the POLARISCO, all the presented data about the November 13, 2015, terrorist attacks in Paris were translated into ontology instances. Then, to query the ontology, we used a SPARQL query editor to check if the proposed ontology can provide the needed information during the operational response. Figure 12 shows an example of the obtained result of the query "Who were the command members of each involved unit in Paris terrorist attacks?". When responding to a disaster, it is key to distinguish the exact role of each involved stakeholder. Accordingly, the command members that were responsible for managing the operational acts on the field are extracted with their specific roles and affiliation. The result of this query illustrates how we can navigate in the stakeholders modules.


```
SPARQL query:
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX RO: <http://www.obofoundry.org/ro/ro.owla#>
PREFIX AO: <http://www.ontologyrepository.com/CommonCore/Mid/AgentOntology#>
PREFIX ERO: <http://www.ontologyrepository.com/CommonCore/Upper/ExtendedRelationOntology#>
PREFIX POLARISCO: <http://www.semanticweb.org/linda/ontologies/2018/11/POLARISCO#>

SELECT DISTINCT ?organization_member ?commandement_role ?organization
    WHERE { ?organization_member AO:supervises POLARISCO:Paris_Terrorist_attacks.
            ?organization_member ERO:has_role ?commandement_role.
            ?organization_member AO:is_affiliated_with ?organization
```

organization_member	commandement_role	organization
Jean_Pierre_Tourtier	Director_of_the_Medical_Response	Healthcare_units
Daniel_Landrieu	Commander_of_Police_Operations	Police
Philippe_Boutinaud	Commander_of_Rescue_operations	Firefighters
Jean-François_Carenco	Director_of_operations	Public_authority

Fig.12. SPARQL query and results of the involved stakeholders and their corresponding command role in Paris terrorist attacks

One of the strengths of the POLARISC system is the generation of the chain of command in order to facilitate information exchange. The organization of the tactical network of communication, known by its French initials OCT, is critical in ensuring the communication among stakeholders at different levels within their respective organizations. Figure 13 depicts an example of the generated OCT of the Paris terrorist attacks.
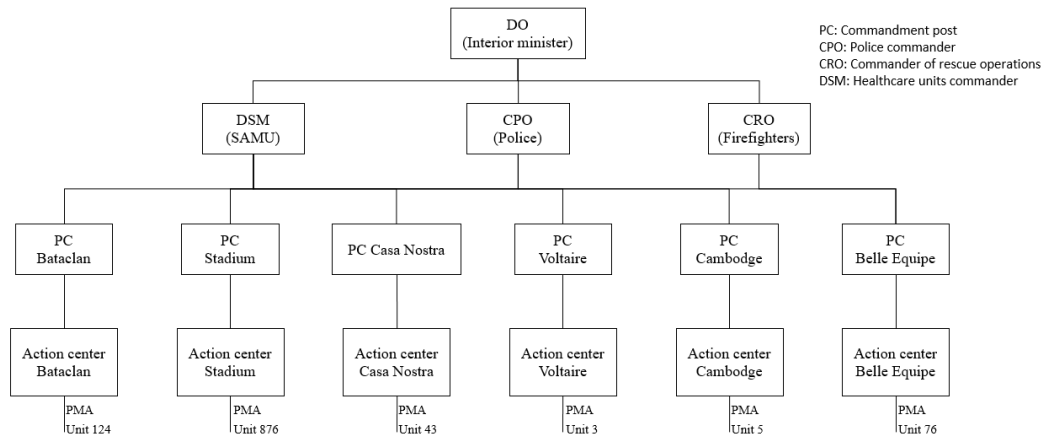
Fig.13. OCT of Paris terrorist attacks

To ensure better communication among the involved stakeholders, POLARISC will support the radio communication tools by the use of the messaging service to enable information tractability and consolidation. To demonstrate the utility of the proposed messaging service, here follows an example of an act of communication among firefighters and health care units as shown in Figure 14. Once the firefighters' unit of the VSAV is on the field, they figure out that they need backup from healthcare units to handle a large number of victims in a critical situation. Let us start to analyze this example of resource-request type message of the firefighters to demonstrate how a communication act can be improved across ERs (Figure 15). First, the term "TA75" remains the same since it is an instance of "pcc: terrorist_attack". Second, VSAV is a subclass of "firefighters' vehicle" and there is no equivalent class with healthcare units module, so we used the annotation of VSAV to explain the meaning of the abbreviation. Then, AE (Absolute Emergency) is a subclass of "firefighters' victim state" which is equivalent to the subclass of "SAMU victim state" P0. Therefore, we substitute AE with P0. Finally, "TA75" took place in the firefighter's action center people succor "AC_PC_75", which is called action center public "P_75" by Healthcare units. Thus, "AC_PS_75" is replaced by "P_75". We can conclude that POLARISCO is the core of the messaging service; it enables semantically enhanced information exchange among different stakeholders. Each stakeholder receives information according to its own semantics.
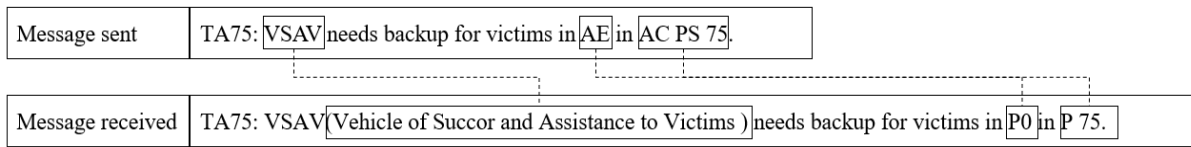
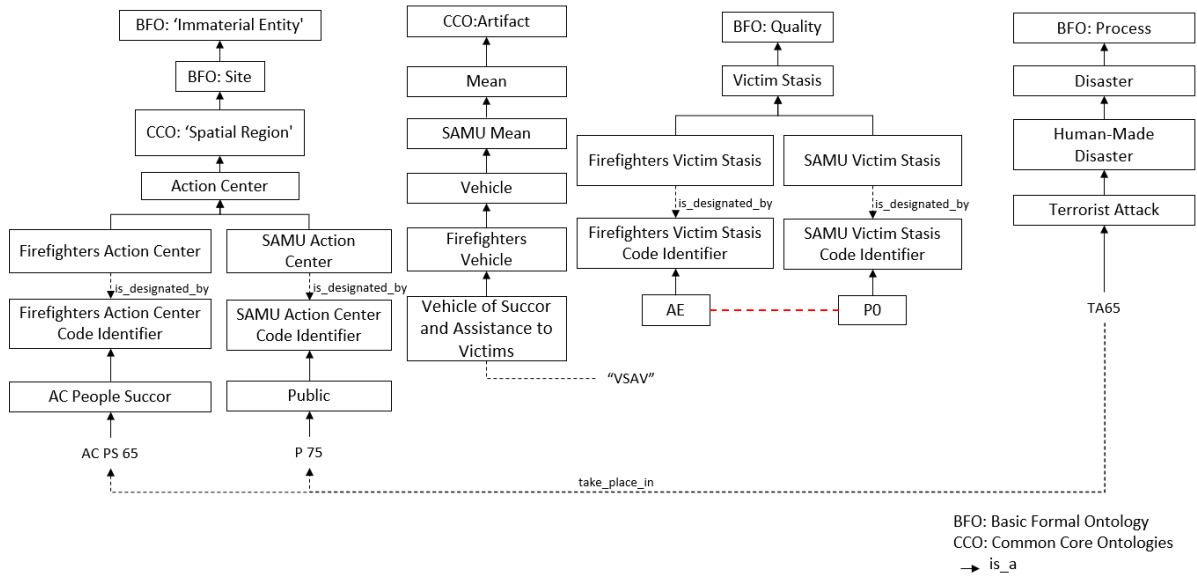| Message sent	TA75: VSAV needs backup for victims in AE in AC PS 75.
Message received	TA75: VSAV (Vehicle of Succor and Assistance to Victims) needs backup for victims in P0 in P 75.

Fig.14. Message transformation example

Fig.15. A sample part of an instance of terrorist attack

VI. Conclusion and Future Work

The larger the disaster is, the more complicated the disaster response becomes. The structure of disaster response is characterized by the multiplicity of the involved actors and their vocabularies. To deal with this diversity, efficient coordination is key, and this requires clear information sharing. We recognized a need for an interoperable multi-level common operational command system based on a common understanding of the meaning of the exchanged data. Therefore, we proposed POLARISC, a novel system that offers to all ERs a real-time operation picture of the situation in order to enable multi-level coordination among EROs including firefighters, police, gendarmerie, healthcare services, and public authorities. It brings together available information in order to consolidate it and to improve information accessibility for ERs. A key element of POLARSIC is the use of the proposed modular ontology, POLARISCO, that defines the knowledge of French emergency response doctrine in order to guarantee a shared and semantically unambiguous information

exchange across ERs. POLARISC responds to all ERs' requirement by guaranteeing timely and accurate data sharing and visualization to ensure effective collaboration and coordination among stakeholders.

In future work, the evacuation, alert, and means management services will be published. Then, an evaluation of the whole system will be conducted through realistic scenario design and exercise. We will be able to test the efficiency of the developed platform in the first exercise planned for 2020.

REFERENCES

[1] Bénaben, F., Lauras, M., Truptil, S., & Salatgé, N. (2016, January). A metamodel for knowledge management in crisis management. In System Sciences (HICSS), 2016 49th Hawaii International Conference on (pp. 126-135). IEEE.

[2] Babitski, G., Bergweiler, S., Grebner, O., Oberle, D., Paulheim, H., & Probst, F. (2011). SoKNOS–using semantic technologies in disaster management software. In Extended Semantic Web Conference (pp. 183-197). Springer, Berlin, Heidelberg.

[3] Barros, R., Kislansky, P., Salvador, L., Almeida, R., Breyer, M., & Pedraza, L. G. (2015). EDXL-RESCUER ontology: Conceptual Model for Semantic Integration. In ISCRAM.

[4] Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. Information Systems Frontiers, 12(1), 49-65.

[5] Boutinaud, B. G. F (2017). Cooperation & Interaction: The Paris Terrorist Attacks. In Norwegian conference for civil protection and crisis management.

[6] Brown, N. J., & Lampen, N. J. (2012). Crisis Management. The Encyclopedia of Human Resource Management: Short Entries, 147-152.

[7] Borretti, C., Degrace, J. N., & Cova, P. (2012). The French Vigilance system. Contributing to the reduction of disaster risks in France. In Institutional Partnerships in Multi-Hazard Early Warning Systems (pp. 63-93). Springer, Berlin, Heidelberg.

[8] Casado, R., Rubiera, E., Sacristan, M., Schütte, F., & Peters, R. (2015). Data interoperability software solution for emergency reaction in the Europe Union. Natural Hazards and Earth System Sciences, 15(7), 1563-1576.

[9] Coste, F., Nexon, E., and Daguzan, JF. (2013) ANVIL: Analysis of Civil Security Systems in Europe, Country Study: France.

[10] Chan, S., Haugh, B. A., Loaiza-Lemos, F. L., Wartik, S. P. (2017). Public Safety and Emergency Management Communications Ontology. IDA Document D-8583

[11] Chen, D., Dassisti, M., & Elvesaeter, B. (2007). Enterprise Interoperability-Framework and Knowledge corpus.

[12] Cinque, M., Esposito, C., Fiorentino, M., Mauthner, J., Szklarski, Ł., Wilson, F., ... & Pignon, J. P. (2015). SECTOR: Secure Common Information Space for the Interoperability of First Responders. Procedia Computer Science, 64, 750-757

[13] Cinque, M., Cotroneo, D., & Fiorentino, M. (2016). Facing reliability requirements for timely information sharing in future crisis management systems. In Fast Abstract in the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.

[14] Clarke, P. (2003). Crisis communications: lessons from September 11. Rowman & Littlefield Publishers.

[15] Dang, J., Hedayati, A., Hampel, K., & Toklu, C. (2008). An ontological knowledge framework for adaptive medical workflow. Journal of biomedical informatics, 41(5), 829-836.

[16] Devlin, E. S. (2006). Crisis management planning and execution. CRC Press.

[17] Elmhadhbi, L., Karray, M. H., & Archimède, B. (2018). An Ontology-based Emergency Response System for Interoperability in a Crisis Situation in Smart Cities. Enterprise Interoperability: Smart Services and Business Impact of Enterprise Interoperability, 421-427.

[18] Elmhadhbi, L., Karray, M. H., & Archimède, B. (2018). Towards an Interoperable Operational Emergency Response System for Large-Scale Situations: POLARISC. ISCRAM 2018

[19] Elmhadhbi, L., Karray, M. H., & Archimède, B. (2018). Toward the use of upper-level ontologies for semantically interoperable systems: An emergency management use case. In Enterprise Interoperability VIII.

[20] Elmhadhbi, L., Karray, M. H., & Archimède, B. (2019). A modular ontology for semantically enhanced interoperability in operational disaster response.

[21] Ghanchi, A. (2016). Insights into French emergency planning, response, and resilience procedures from a hospital managerial perspective following the Paris terrorist attacks of Friday, November 13, 2015. Disaster medicine and public health preparedness, 10(5), 789-794.

[22] Gruber, T.R. (1995). Toward principles for the design of ontologies used for knowledge sharing? International journal of human-computer studies, 43(5-6), 907–928.

[23] Havlik, D., Pielorz, J., & Widera, A. (2016). Interaction with citizens' experiments: from context-aware alerting to crowdtasking. In ISCRAM.

[24] Homeland Security (2016). National Response Framework. Third Edition.

[25] IEEE, (1990) IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries.

[26] Ide, N., & Pustejovsky, J. (2010). What does interoperability mean, anyway? Toward an operational definition of interoperability for language technology. In Proceedings of the Second International Conference on Global Interoperability for Language Resources. Hong Kong, China.

[27] Iannella, R., Robinson, K., & Rinta-Koski, O. (2007). Towards a framework for crisis information management systems (CIMS). In Proceedings of the 14th Annual TIEMS Conference.

[28] Jensen, J., & Thompson, S. (2016). The incident command system: a literature review. Disasters, 40(1), 158-182.

[29] Kean, T. H., & Hamilton, L. H. (2004). The 9/11 Report. New York: St. Martin's Press.

[30] Kristiansen, E., Johansen, F. H., & Carlström, E. (2019). When it matters most: Collaboration between first responders in incidents and exercises. Journal of Contingencies and Crisis Management, 27(1), 72-78.

[31] Lagadec, P. (2002). Crisis management in France: trends, shifts, and perspectives. Journal of contingencies and crisis management, 10(4), 159-172.

[32] Li, T., Xie, N., Zeng, C., Zhou, W., Zheng, L., Jiang, Y., ... & Chen, S. C. (2017). Data-driven techniques in disaster information management. ACM Computing Surveys (CSUR), 50(1), 1.

[33] Lindell, M. K., Perry, R. W., & Prater, C. S. (2005). Organizing response to disasters with the incident command system/incident management system (ICS/IMS). In International workshop on emergency response and rescue (pp. 1-6).

[34] Manoj, B. S., & Baker, A. H. (2007). Communication challenges in emergency response. Communications of the ACM, 50(3), 51-53.

[35] Mhadhb, L., Akaichi, J., Karray, M. H., & Archimde, B. (2015, April). Ontologies for location based services quality enhancement: the case of emergency services. In 2015 Second International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 90-97). IEEE.

[36]Shaluf, I. (2007). Disaster types. Disaster Prevention and Management: An International Journal, 16(5), 704-717.

[37]Nossiter, A. (2015). Response to Paris Attacks Points to Weaknesses in French Police Structure. In the New York Times.

[38]Nikolai, C. M., Johnson, T., Prietula, M., Becerra-Fernandez, I., & Madey, G. R. (2015). Design Principles for Crisis Information Management Systems: From Closed Local Systems to the Web and Beyond. International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 7(4), 26-45.

[39]Philippe, J. M., Brahic, O., Carli, P., Tourtier, J. P., Riou, B., & Vallet, B. (2016). French Ministry of Health's response to Paris attacks of 13 November 2015. Critical Care, 20(1), 85.

[40]Salmon, P., Stanton, N., Jenkins, D., & Walker, G. (2011). Coordination during multi-agency emergency response: issues and solutions. Disaster Prevention and Management: An International Journal, 20(2), 140-158.

[41]Schäfer, C., Sauerland, T., Pottebaum, J., Marterer, R., Behnke, D., Wietfeld, C., ... & Despotov, B. (2017, April). Cloud-based semantic services for Pan-European emergency preparation and planning. In Systems Conference (SysCon), 2017 Annual IEEE International (pp. 1-7). IEEE.

[42]Sena, L., & Michael, K. W. (2006). Disaster prevention and preparedness. Ethopia Public Heal Train Initiat, 1, 1-180.

[43]Smith, J. M. (2012). Comprehensive Common Operating Picture (COP) for Disaster Response (No. ATZL-SWV). Army Command and General Staff Coll Fort Leavenworth Ks School of Advanced Military Studies.

[44]Song, F., Zacharewicz, G., & Chen, D. (2013). An ontology-driven framework towards building enterprise semantic information layer. Advanced Engineering Informatics, 27(1), 38-50.

[45]Stambler, K. S., & Barbera, J. A. (2011). Engineering the incident command and multiagency coordination systems. Journal of Homeland Security and Emergency Management, 8(1).

[46]Three Levels of War (1997). USAF College of Aerospace Doctrine, Research and Education (CADRE) Air and Space Power Mentoring Guide, Vol. 1 Maxwell AFB, AL: Air University Press.

[47]Vidan, A., & Hogan, G. (2010, November). Integrated sensing and command and control system for disaster response. In 2010 IEEE International Conference on Technologies for Homeland Security (HST) (pp. 185-189). IEEE.