Munk Sándor

EMERGENCY AND HOMELAND SECURITY INTEROPERABILITY QUESTIONS IN THE USA

Abstract

In our days the handling of situations due to natural and technological disasters, or acts of terrorism requires successful and efficient cooperation of numerous different organizations. Activities of these organizations now are growingly supported by IT systems and devices. An essential condition of the efficient cooperation is the seamless, interoperable information exchange between/among their IT systems. This publication introduces and analyses the interoperability problems and solutions in the field of incident, and emergency-handling, and homeland security in the USA.

Napjainkban a természeti és technológiai eredetű katasztrófák, terrorcselekmények következtében kialakult helyzetek kezelése számos különböző szervezet eredményes és hatékony együttműködését igényli. Ezen szervezetek tevékenységét ma már egyre bővülő mértékben segítik informatikai rendszerek és eszközök. A szervezetek közötti hatékony együttműködés alapvető feltétele az informatikai rendszereik közötti rugalmas, interoperábilis információcsere. Jelen publikáció bemutatja és elemzi katasztrófavédelem és a rendvédelem során az Egyesült Államokban felmerült interoperabilitási problémákat és megoldásokat.

Keywords*: information interoperability, emergency management, information exchange languages ~ információs interoperabilitás, katasztrófavédelem, információcsere nyelvek.*

INTRODUCTION

In our days the defense sector functions – homeland security, border security, emergency management, critical infrastructure protection, defense against terrorism – are increasingly depend on the available information and the services of different IT systems. Although the level of IT support provided for the different application areas is continuously higher, at the same time new problems have appeared and cause continuously growing troubles in the field of information sharing between supported organizations, and in information exchange between/among their IT systems.

Much of the information necessary for different activities exists in disparate databases scattered among different IT systems of different organizations. In many cases these IT systems cannot exchange, share information neither horizontally (with partner organizations on the same level), nor vertically (between local, regional, and central organizations). Moreover in the defense sector information exchange is usually necessary not only in a national framework, but in an alliance. For example, in the case of Hungary the European Union, or other environments.

In the relevant literature we can find numerous problem types of information exchange, and information sharing in the defense sector. Certain government agencies storing terrorist information, such as terrorist "watch lists" have not been able to systematically share that in-

formation with other agencies. This situation sometimes results in errors, for example visa applications and border controls are not checked against consistent "watch lists". Even member states of a federal state maintain terrorism, gang, and drug databases that other states cannot access. Communication equipment and procedures used by different organizations are often incompatible. So traditional and wireless communication systems of these organizations cannot be connected, they cannot communicate with their counterparts during incidents.

At the beginning of the 21st century the problems of information exchange between heterogeneous IT systems highlighted the questions of information interoperability (above all the interconnection of communication systems, and the commonly agreed, and consistently interpreted information exchange data formats) in the defense sector too. In the following we will introduce, and analyze some interoperability ideas, and solutions used in this field. These are from the USA, due to its leading role in IT application, as well as to some serious, even tragical natural disasters, and especially the 9/11 terrorist attack in 2001.

1. COMMON ALERTING PROTOCOL

In the United States of America, the first interoperability solution in the field of disaster management has appeared as a consequence of a working group report [1]. According to one of the report's recommendations "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally, and nationally for input into a wide variety of dissemination systems" [1, p 7]. To implement the recommendation, the development of a standardized alerting message format has begun in 2001.

The Common Alerting Protocol (CAP) is a communication method independent, XML-based standardized message format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. The first version of the message format was approved as an international standard in 2004 [2], and in 2005 a modified version (CAP 1.1) was also accepted.

During development of the CAP message format some critical application requirements were formulated [3]:

"1. Warning messages need to be coordinated over multiple delivery systems, both to reach the greatest number of people at risk with the greatest reliability, and let the public be confident that they've received a legitimate warning and not just a false alarm over one particular system;
2. Effective warnings contain all the information people at risk need to evaluate situations and take appropriate actions. The essential elements of a warning include the location, timeframe, severity, and likelihood of the hazard, along with clear and reliable information about the source of the warning and what people at risk can do to protect themselves; and,
3. Warnings need to go to the people at risk and not to people who aren't affected; in other words, effective warnings are 'targeted' to the right people at the right time."

The CAP message format is based on four essential components, the so called segments [4]. Each CAP Alert Message consists of an 'alert' segment, which may contain one or more 'info' segments, each of which may include one or more 'resource', and 'area' segments. The 'alert' segment provides basic information about the current message: its purpose, its source and its status, as well as it is a unique identifier for the current message and links to other, related messages. An 'alert' segment may be used alone for message acknowledgements, cancellations or other system functions, but most 'alert' segments will include at least one 'info' segment.

An 'info' segment describes an anticipated or actual event in terms of its urgency (time available to prepare), severity (intensity of impact) and certainty (confidence in the observation or prediction), as well as providing both categorical and textual descriptions of the subject event. It may also provide instructions for appropriate response by message recipients and various details (hazard duration, technical parameters, contact information, links to additional information sources, etc.).

The 'resource' segment provides an optional reference to additional information related to the 'info' segment within which it appears in the form of a digital asset such as an image or audio file. The 'area' segment describes a geographic area to which the 'info' segment in which it appears applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred representations use geospatial shapes (polygons and circles) and an altitude or altitude range, expressed in standard latitude / longitude / altitude terms.

Authenticity and security of CAP messages can be ensured by XML based digital signature and encryption methods.

A single CAP message can be used as a unique source to activate (trigger) different alerting and public information systems, such as: sirens, technical emergency alert systems, internet news feeds, e-mail alerts, highway sign messages, television text captions, and automated telephone calls, or radio broadcasts.

In 2004, based on the success of CAP, the Federal Emergency Management Agency and the emergency preparedness and response branch of the Department of Homeland Security formed a partnership with the Emergency Interoperability Consortium to develop an expanded family of data formats (EDXL) for exchanging operational information beyond warning.

2. EMERGENCY DATA EXCHANGE LANGUAGE

The Emergency Data Exchange Language (EDXL) is a family of XML-based information exchange specifications that is intended as an "umbrella" for a number of emergency data message types including incident notification and situation report, status reporting, resource requests and dispatch, exchange of analytical data and geospatial information, identification, and authentication.

The project comprises three layers. The EXDL Vocabulary contains specialized data elements and taxonomies to apply common terminology to data sharing regarding emergency incidents, conditions, resources, activities and outcomes. This will draw heavily on current common-vocabulary efforts, and appropriate XML standards. EXDL Messages include formats for messages (XML documents) using EXDL Vocabulary to implement emergency messages. At last EXDL Interfaces are technical protocols and formats for routing EXDL messages over various kinds of data networks and systems, based on SOAP and web-service standards, but generalized for use in a wide variety of communication environments.

The EXDL Distribution Element is the key element of the EXDL message format family. Its primary purpose is to facilitate the routing of any properly formatted XML emergency message to recipients. The Distribution Element may be thought of as a "container". It provides the information to route "payload" message sets (such as alerts, or resource messages), by including key routing information such as distribution type, geography, incident, and sender/recipient IDs.

The planned, and already identified standard message sets carried by Distribution Element will be the following: alert message set (identical with the CAP messages), resource message set (to request, or respond to requests, for persons and things required in emergencies), geo-

graphic information messages (to identify, track, trend, or forecast events and resources; to establish the geospatial context; to communicate about geographic features and things), situation status messages (for reports providing the overall status of an event and the subsequent emergency response), finally other specific message sets (according to the practitioners arising needs). From the components only the CAP message set and the Distribution Element were accepted as an international standard up to 2006. [5]

3. GLOBAL JUSTICE XML DATA MODEL, NATIONAL INFORMATION EXCHANGE MODEL

Global Justice XML Data Model (GJXDM) is an XML-based standard data model designed specifically for criminal justice information exchanges, for providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch. The first two version of the data model were data dictionaries containing data elements, used in justice-related information exchange.[1] In 2003 a working group began to create a more comprehensive product that included a data model, a data dictionary, and XML schema generated from these. The total package became known as Justice XML Data Model, and later the Global attribute was added. The first four prereleases of GJXDM 3.0 were published in 2003.

The GJXDM directly doesn't define sets of data for particular organizational information exchanges. So given the same set of organizational data requirements, without prior agreements, albeit based on the same standardized and commonly interpreted GJXDM data elements, each implementing organization would like to come up with a different information exchange format for similar purposes. For example each state in the USA may develop an own GJXDM format of an Arrest Report. So there could be 50 or more instances of Arrest Report formats, each potentially having legitimate differences due to unique requirements of each state. However most differences will likely be arbitrary and unnecessary. But a reference Arrest Report format developed as a result of a federal level harmonization may be a good basis (template) for states to extend with local specialties. To solve this problem the GJXDM XML Structure Task Force created the concepts of 'Information Exchange Package' and 'Reference Information Exchange Packet'. Up to 2006 more than hundred of these packages were developed.

Leveraging the GJXDM results and efforts the Department of Homeland Security and the Department of Justice launched a new extended interoperability solution (NIEM) to facilitate timely, secure information sharing across the whole of the justice, public safety, emergency and disaster management, intelligence, and the homeland security areas.

According to an official document [6] "a variety of emergency situations in recent years have demonstrated in increasingly vivid detail the tragic consequences that often result from the inability of jurisdictions and agencies to affectively share information. Terrorist attacks, natural disasters, and tragic large scale criminal incidents too often serve as case studies that reveal weaknesses in our nation's information sharing infrastructure". "Even though agencies perform similar operational functions, their internal business processes are inconsistent, and they continue to use different information systems and technology support them." "As a consequence, these agencies are unable to effectively share information in a timely, secure manner, and too often, there are fundamental differences in the nature and understanding of information between them."

National Information Exchange Model is a compound of a GJXDM-like XML-based data model, the appropriate data dictionary, the information exchange packages (message formats)

[1] Reconciliation Data Dictionary (RDD), Justice XML Data Dictionary (JXDD).

used during information sharing between organizations, and a set of operational processes and procedures. The purpose of NIEM is to support interoperable information exchange between communities of interest (domains) across all levels of government. As a consequence, not all data needs to be NIEM-compliant, only the data that is being shared across domains. The first domains identified, were the following: justice, intelligence, immigration, emergency management, international trade, critical infrastructure protection, and information assurance. These can be extended in the future to healthcare, and transportation.

All NIEM data elements are classified according to three categories. [6, p 7] Data components, commonly shared and understood among all domains are identified as universal components (e.g. person, address, organization, contact, activity, vehicle), while components used in exchanges between multiple domains but not universally shared, are identified as common components (e.g. offense, sentence, and disposition). Components managed by a specific community of interest (e.g. appellate case decision, and arrest agency) are considered domain specific. These later can be further divided into federal, state, local, and tribal levels, built on top of one another.

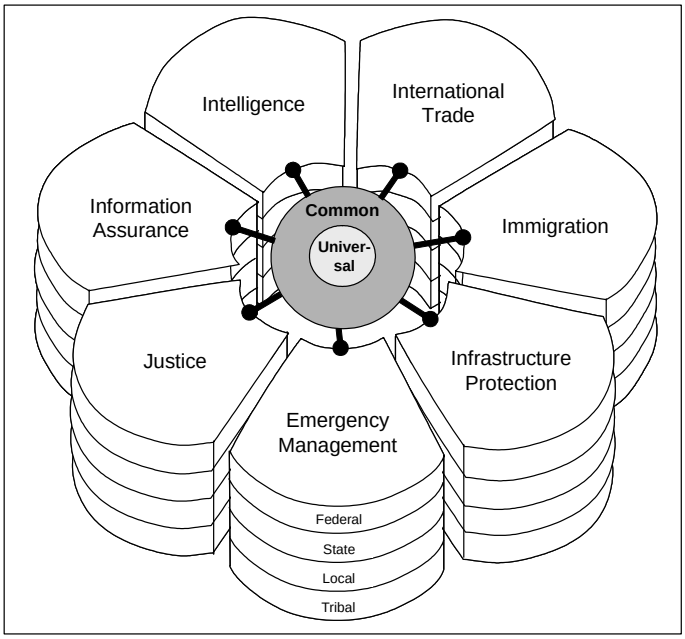

Figure 1: NIEM Component Architecture [6, p 8]

NIEM does not attempt to 'normalize' all information systems or standards across relevant domains. It wants to identify operational information exchanges among participating domains by examining current practice (i.e. documenting business requirements for information exchange between agencies and domains) and by modeling new and innovative information exchange opportunities to achieve greater efficiency, effectiveness, return on investment, and new operational capabilities. Not all information an organization collects needs to be shared with other organizations or domains. Identifying precisely what information is exchanged between organizations can be best determined by modeling relevant organizational practices of the domains through scenario-based planning and information exchange mapping.

Scenarios describe the organizational context of events, incidents, or circumstances in which information must be exchanged between agencies and/or domains. Such scenario may be a terrorist attack on a city, a natural disaster, a major criminal incident requiring response by multiple agencies or jurisdictions, or simply the day-to-day operations of justice, public safety, and homeland security agencies at all levels of government. Careful elaboration of organizational scenarios can identify critical operational points at which information must be

shared between two or more parties for effective prevention, response, and remediation. Using scenario-based planning, communities of interest can document their organizational requirements and complete their information exchange mapping and modeling, and make proposals to extend NIEM.

SUMMARY

Concept of interoperability, meaning a mutual capability for successful and efficient cooperation, is inseparable from the concept of heterogeneity, because among every respect homogenous cooperating parties there can not be interoperability problems. Regarding information interoperability heterogeneity can appear in concepts, information contents, information representations, and technical devices applied by the parties.

In military application questions of information interoperability appeared in the 1950s, and in the field of emergency management and law enforcement at the beginning of the 21st century. Basic reasons for their appearance are the growth of the level and role of efficient cooperation between autonomous organizations, and the ever extending application of IT systems, and services. In case of traditional information exchange without use of technical devices heterogeneity has appeared in the concepts, languages, and symbols. These differences were handled by human knowledge (by knowledge of other thinkers, foreign languages, and notation systems).

First interoperability problems appeared in the case of cooperating parties using heterogeneous communication systems, devices, and procedures. Interconnection of different voice-oriented systems was basically a technical task that did not directly affect the users. Technological development in this field brought significant results. Today there are no conceptual obstacles to the interconnection of different communication systems. In the common application area a worldwide interoperable communication network has been evolving. On the other hand in the case of communication systems developed for special (e.g. military, emergency) application environments interconnection in general has not been achieved yet.

The second group of interoperability problems is connected to data exchange between IT systems of cooperating parties. Certain problems, particularly the differences in the information representations (data exchange protocols, formats) can be relatively easily handled, such as in the case of technical interoperability questions. Development of standardized and agreed solution is easier, because the participants do not care about the formats being used during information exchange. They have only requirements regarding the 'expressive power' of the formats, and the efficiency parameters (e.g. speed, security, or size) of information exchange.

Based on the questions introduced earlier it can be stated, that the development of standardized intermediary representations in the field of emergency management and homeland security has happened similarly to other fields of application. The first solutions had appeared in narrower application areas, and later were gradually extended – sometimes by integration – to wider areas. This process was in strong connection with, and determined by the volume and closeness of cooperation, and information exchange.

Analysing the experiences it seems to be obvious that the development of intermediary representations designed for wider, and wider application requires more and more preliminary discussions and time. It will also likely be accompanied by more and more difficulties, since a wider application area involves more significant differences in the conceptual systems, and in the interpretations of the same information. Another difficulty, left to the cooperating parties, is the conversion between the inner representations and interpretations, and the intermediary information exchange format.

The main conclusion is that the real interoperability problems, related to the meaning and concepts in the field of emergency management, homeland security, and other areas are still ahead of us. These problems can not be solved by technical solutions only, but also require a lot of subject matter expertise as well as a high level of knowledge.

REFERENCES

[1] *Effective Disaster Warning. Report by the Working Group on Natural Disaster Information Systems.* Subcommittee on Natural Disaster Reduction, November 2000.

[2] *OASIS* [Organization for the Advancement of Structured Information Standards] *200402, Common Alerting Protocol v1.0.* March 2004.

[3] *CAP Cookbook. – A Roadmap to Emergency Data Standards.* [http://www.incident.com/cookbook/index.php/A_Roadmap_to_Emergency_Data_Standards, downloaded on 2006.08.08.]

[4] *Common Alerting Protocol v1.1.* OASIS Open, 1 October 2005.

[5] *OASIS, Emergency Data Exchange Language (EDXL) Distribution Element v1.0.* May 2006.

[6] *Introduction to the National Information Exchange Model (NIEM). Document Version 1.0.* NIEM Program Management Office, June 30, 2006.