"INFORMATION GRID IN SUPPORT OF CRISIS MANAGEMENT"

Dr. Eldar Aarholt (PhD), Mr. Olav Berg (MSc)
Teleplan AS, P.O.Box 69, 1324 Lysaker, Norway[1]

Abstract

This paper deals with information availability related to crisis management, an area that has become a prioritised national and international concern. The paper looks into two different scenarios with a view to identify some shortcomings and possibilities inherent in a national information infrastructure. By fairly simple means it is possible to obtain significant improvement of data availability, which in turn will give a substantial contribution to improved emergency preparedness through the availability of a national crisis information grid. A network centric solution is suggested, where the limitations inherent in today's information grid are overcome, and where information is dynamically made available as required.

1 INTRODUCTION

With western societies becoming increasingly dependent upon modern infrastructures, they are also becoming more vulnerable, since disturbance to any of these infrastructures usually will influence a large number of people. Crisis Management (prevention and handling) becomes a prioritised national and international concern. This paper looks into two different scenarios with a view to identify some shortcomings and possibilities inherent in a national information infrastructure. By fairly simple means it is possible to obtain significant improvement of data availability, which in turn will give a substantial contribution to improved emergency preparedness through the availability of a national crisis information grid. In the following cases Norway is used as an example. However, the presented examples and findings would be typical for many small nations.

When considering national crisis management, some bodies will be the main contributors to the information grid. These can further be sectioned into the following groups as seen in Table 1.

Community infrastructures	Information contributors
Communications	Telephone, data, video
Energy supplies	Electricity, oil, natural gas
Food supplies	Supermarkets, imports,
Law and order	Military, police, fire
Media	TV, newspapers, magazines
Medical	Acute medicine, health care
Transportation	Road, air, train, ship

Table 1. Community infrastructures and relevant information contributors

[1] E-mail addresses: aar@teleplan.no (Eldar Aarholt) and ob@teleplan.no (Olav Berg)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Grid in Support of Crisis Management	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Teleplan AS,PO Box 69,1324 Lysaker, Norway, ,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**11**	

Each one of these bodies can be a data provider, a data user or ideally both to a national information grid. The following two scenarios are considered:

- Interruption of the European Gas Supply
- Environmental crisis caused by man

This paper considers the possibilities and benefits by introducing an *"Information grid in support of crisis management*", or in other words a *"Network based crisis management concept*". The crisis management process, concerned infrastructure and data availability in relation to the above incidents are discussed.

2 THE CRISIS MANAGEMENT PROCESSES

An incident is likely to be of considerable scale for it to be called a crisis, and a crisis must be quite major to be called a national catastrophe. The definition of a national catastrophe varies over time:

> *Nowadays, in the order of fifty deaths can be a national catastrophe.*
>
> *In the world wars, that many died every few seconds…*

Searching the Internet for "*national catastrophe*" lists a number of well-known incidents, such as:

- The oil crisis in 1973 – the oil price rocketed from $7 to $25 per barrel
- Chernobyl – the nuclear accident in 1986

It is fair to say that the success in dealing with these crises was varied.

The top-level value-added processes in relation to crisis management can be structured as follows:

Figure 1. Crisis management main value-added processes

Beneath each of these main actions lies a command level where responsibility is placed; that is, "*who shall do what*", which in turn triggers the various operational actions and procedures. There is no major functional difference between a military and a civil crisis management system. The quality at which each action is performed relies strongly on the availability of precise and timely data.

2.1 THE INFORMATION CRISIS

In the event of a rising crisis, some seemingly unrelated events may lead to a serious escalation of the crisis. For example, the lack of precise and timely information during a crisis will, most likely, change the outcome of an ongoing crisis to the worse by an inability to carry out some of the main crisis management actions listed above. This condition is called an information crisis, and it can be divided into six different types as follows:

> **Fear crisis**: A large and acute public need for information due to a massive uncertainty of what has happened, where did it happen, who are involved, what is the cause, and what are the after-effects.
>
> **Stress crisis**: The news channels are unable to meet high demands for information through their usual communications routines. Communications between official bodies

and the public is put under pressure and can – at times – break down completely. This can be due to a huge public activity that can block the usual communication channels, for example the telephone exchanges or stress the people set to answer questions.

Decision crisis: Unclear lines of responsibility are experienced with lack of overview and coordination. The uncertainty consists of who has and who can provide correct and timely information.

Comprehend crisis: The experts may disagree on the state of affairs, how it is developing and what should be done. Science need not be hard facts and exact knowledge, but rather conflict of hypothesis and polemics. The alternatives that appeal to the scientists may intimidate and scare the public who are in doubt as to who or what to believe.

Confidence crisis: A disagreement between an official body and the public resulting in criticism of inadequate and late information.

Legitimacy crisis: A disagreement between an official body and the media, resulting in accusations of lack of credibility and confidence. The official body may be considered incompetent, which in turn amplifies the information crisis. The relayed messages may not be taken as facts, but as speculative assertions and doubtful suggestions. This may lead to even more information being used from less credible sources.

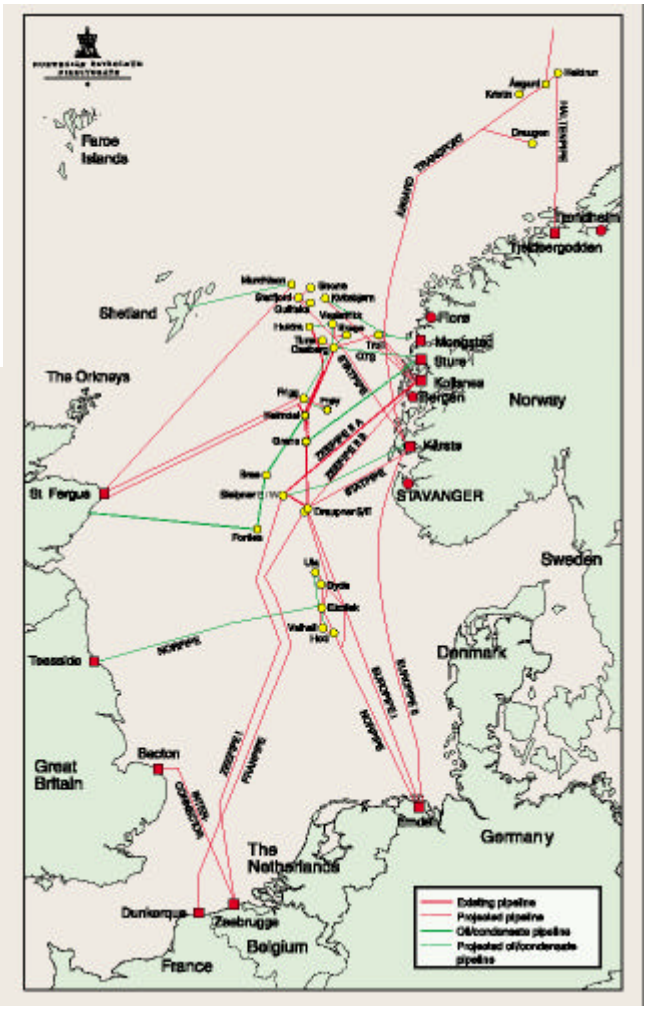
These types of information crisis are recognised as being an important component in the scenarios described later in this paper.

2.2 CRISIS MANAGEMENT SCENARIOS

2.2.1 Scenario 1 - Interruption of European Gas Supply

The first scenario deals with the supply to the European natural gas market. In 2000 Europe used 430 billion cubic metres of natural gas, and environmental policy decisions and new technologies will increase the demands in the years ahead. Considering that the increased supply must come primarily from imports and that the European Union (EU) as a whole is served by an integrated pipeline system as illustrated in Figure 2, the greatest risk is that of supply interruption in a major pipeline from outside the EU. This could result from political instability in the producer country or in a country that is transited by the pipeline. The problems of supply cause providers to reinforce existing national efforts to diversify their individual supply sources and to address problems of security of supply.

Norway is one of a few important suppliers to the European gas market. Its national public services with associated information and management systems have an organisation and status that is representative for most of the important providers to the market. The Norwegian Ministry of Petroleum and Energy administer the legislation, concession and control of the national oil and gas sectors. Other important participants in relation to crisis prevention and handling are the Norwegian Air Traffic and Airport Management, the National Coastal Administration and the Norwegian Defence. As a whole, these bodies manage information systems of high relevance to crisis management. An integration of these systems into a National Crisis Information Grid would give a significant contribution to an increased security in the distribution of natural gas supply in Europe.



The operators are responsible for the safety of the production of oil and gas even if threats of terror and sabotage exist. The police have the authority and responsibility to deal with the source of the threat. In most situations the Police will have to be assisted and reinforced by military (special) forces that will bring and be supported by their own command and control system. The Coastguard is also obliged to give assistance to the Police in such situations, but the Norwegian Special Forces are the only national element with capabilities and resources to conduct extensive operations at installations at sea.

Several costal radars and radars located on offshore installations cover parts of the petroleum production within the national economic zone and territorial waters. However, the data from these radars are not merged into one picture and are only available to local users.

Together with NATO, the Norwegian Armed Forces is the owner of sensors capable of covering the whole area of operation. The Police have no access to military systems and thereby vital surveillance data. This results in troublesome transfer of information, difficult coordination and low response times.

Figure 2. Pipelines and land facilities[2] (Scenario 1)

2.2.2 Scenario 2 - Environmental Crises

This scenario deals with the development of environmental catastrophes on a national level. These are almost always caused by man and brought on by a failed industrial venture. Examples can be the radioactive contamination and after-effects caused by the Chernobyl reactors in 1986, pollution from highly industrialised areas distributed to other regions as acid rain, or even the socio-economical consequences of addiction of harmful substances, such as drugs and alcohol.

Radioactive pollution of our environment may cause severe health problems, and some potential sources of radioactive pollution in Europe are shown in Figure 3. Potential benefits from increased data availability in this area are investigated in this paper. The Norwegian Radiation Protection Authority (NRPA) carries out annual monitoring of nature, food and radiation doses received by the population in order to chart the concentrations of radioactivity and follow trends over time. The

[2] Source: Ministry of Petroleum and Energy (2002) – Fact Sheet 2002 Norwegian Petroleum Activity

challenge becomes that of not only reporting the actual environmental crisis, but to monitor and report on the less obvious consequences. This involves fusing data from a wide variety of socio-economical areas, a process that would benefit from the existence of a national crisis information grid.

Figure 3. Potential sources of radioactive pollution[3] (Scenario 2)

2.2.2.1 Nature (Radiation Fallout) Warning System

The Chernobyl accident occurred around 01:30 on 26. April 1986. Eleven hours later, national news correspondents in Scandinavia reported that a measurement station had detected radioactive fallout; reason unknown. The contamination was distributed to neighbouring countries by local winds. It took weeks to understand the impact of the disaster. Most of the damage has been and is being done to the Republic of Belarus, which has received 75% of the Chernobyl radiation. The total release of the radioactive substances[4] was estimated to about 2,500 times that of the *Windscale* nuclear plant accident in England in 1957, and 16 million times that of the *Three Mile Island* incident in Pennsylvania in 1978.

Political willingness to inform would be the quickest channel to report a nuclear accident. If that willingness were absent, then neighbouring countries would need to rely on own radiation measurement stations. The consequence would be inactivity brought on by a long time lag, as experienced in the Chernobyl accident.

A crisis management team must react immediately to limit loss of lives. Especially the alert and evacuate actions are essential in this context. A sensible configuration of radiation sensors would be to interconnect them to the information grid for public Internet access to allow anyone to subscribe to the data in an effort to reduce the public fear factor. This is of course not the cure in the case of a nuclear accident, but it would alleviate the stress crisis as well as the fear crisis through availability of vital data in the event of a nuclear accident.

[3] Source: Ministry of Petroleum and Energy (2002) – Fact Sheet 2002 Norwegian Petroleum Activity
[4] "Chernobyl - Ten years on", Radiological and health impact, An assessment by the NEA Committee on Radiation Protection and Public Health, OECD Nuclear Energy Agency, November 1995

2.2.2.2 Food Warning System

Since the Chernobyl disaster, radioactivity monitoring in Norwegian food has received a lot of attention. This work is performed as a collaborative venture by the Norwegian Food Control Authority, the Ministry of Agriculture and the Norwegian Radiation Protection Authority, and is called LORAKON. The network comprises 59 stations that regularly measure radioactivity in food and undertake random sampling at slaughterhouses.

The Norwegian Radiation Protection Authority, financed by the Ministry of Fisheries, initiated systematic monitoring of Norwegian fish. In 1999 this was expanded into a marine monitoring programme, financed by the Ministry of the Environment, to chart trends in radioactive pollution of water, sediments, fish and other important marine species. In addition the Fisheries Directorate, the Norwegian Food Control Authority cooperate in a monitoring programme for radioactivity in fish.

2.2.2.3 Population Warning System

In Norway the population can be alerted by a countrywide civil defence warning system configured to sound three basic messages; "*air attack*", "*all-clear*", and "*important message – listen to the radio*". The system is primarily designed for air attack warning at times of war, and as such, not designed to deal with information intensive catastrophes.

Alternate networks may complement this basic means of communications, for example mobile telephone networks and computer networks such as Internet. Nearly every person in Norway owns a mobile phone or works on a computer connected to the Internet.

In the case of a local catastrophe, the alert signal can for example easily be sent as text messages to all mobile phones camping on the mobile phone base stations located within a certain area. The mobile phone operators have access to up-to-the-minute information of who is connected and where they are located. The use of mobile phone connectivity information has a great potential as a mass alert part of a crisis management system, as long as the ether is intact. However, the required subscriber information is presently unavailable for crisis management use.

2.2.3 Radioactive Crises Management System

The Chernobyl accident resulted in widespread nuclear pollution in Norway, with need for extensive countermeasures. The accident highlighted the need for nuclear accident preparedness and competent scientists even in a non-nuclear nation. Public concern has increased significantly. Since the dismantling of the Soviet Union, the Norwegian insight into Russian environmental problems has increased tremendously. Huge problems with civil and military nuclear installations, radioactive waste, and disintegration of security systems have been identified, and have been debated in the newspapers.

In emergency situations, the information is coordinated through the Crisis committee of the nuclear emergency preparedness system. This is a system coordinating several ministries and agencies relevant for nuclear emergencies, and is headed and operated by NRPA. The Crisis committee is authorized not only to inform, but also to decide the content of the coordinated information from all participating agencies. This is to avoid the confusing media situation as seen after the Chernobyl accident, where different agencies issued different evaluations and statements.

A centralised crises management concept is established, however, manual coordination and information exchange among the participating agencies themselves and towards other relevant

parts of society makes reaction times longer than necessary. This includes handling of information from potential and existing warning systems. Furthermore, sources of information have to be predefined, which limits a dynamic adaptability that in certain circumstances would have been beneficial. The next section deals with an information concept that would improve information awareness in relation to crisis management.

3 NETWORK CENTRIC CRISIS MANAGEMENT CONCEPT

In the commercial sector, dominant competitors have developed information superiority and translated it into a competitive advantage by making the shift to network-centric operations. Similar concepts are beginning to take root in military thinking, new concepts, plans, and experiments. It is for this reason that developments in the commercial sector are significant and worthy of note, for they provide insights into the potential power of information superiority in the conduct of military operations.[5]

Crises management on a national (and international) level faces many of the same challenges as seen related to future military operations. It is therefore likely that arguments for network centric solutions can be found from the same set of arguments.

3.1 VITAL BUSINESSES (PUBLIC AND PRIVATE SECTORS)

Today's society faces a wide variety of threats. At one hand of the scale the challenges can be extensive security political crisis and war. The challenges at the other hand of the scale – experienced during more normal and peaceful circumstances - have a varied set of components. One component can consist of the well-known types of natural disaster or "*act of God*", accidents or technical breakdowns and that strikes unpredictable and random. This is probably the dominating component. But also during normal peaceful conditions strikes, from fundamentalists can occur. These kinds of challenges are usually associated with terrorism.

Vital services are interwoven and produced across the public and private boundaries. Events that disrupt these services can arise from a wide spectrum of threats. Triggers of these events represent threats against the society or nation as a whole. A graphical illustration of this is given in Figure 4.

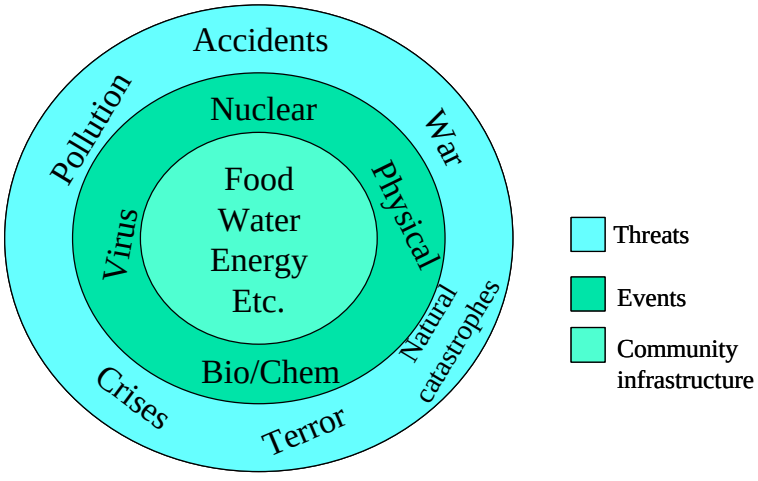


Figure 4. Relationship between threats, events and important infrastructures

[5] Understanding information age warfare (2001) / David S. Alberts [et al.].

The technological advances, especially for computer- and information systems, have provided new ways of solving tasks. This has led to a fundamental restructuring of the entire society. The use of new technology is channelled partly towards more effective and thereby more profitable solutions of known tasks, and partly towards solving new tasks and marketing of new services and products. Information- and communication technology gives more effective decision processes, better overview over systems, and more effective distribution systems. The technology is also a tool for a more open society with increased insight and availability to the public.

Technological development and globalisation are strong driving forces for a continued welfare expansion. However, the large changes to society have led to very complicated and interrelated organisations, and it has at the same time reduced the local governmental influence. The different main functions in society – such as transport, energy, communications and health services – have developed a great deal of mutual interdependence as illustrated in Figure 5. The effect of this means that a failure of one of the above functions often will lead to negative spill-over effects in other areas of the society. This is especially the case for telecommunications, information- and communications technology and energy supplies.

A list of vital businesses, as seen from a functional point of view could become quite extensive. Even though, basic public services related to areas like health, transportation, and water, is still obvious to include, modern societies can stop functioning from breakdown within a lot of other, not so obvious areas as well. Given from the scenarios presented in this paper and some additional studies, we find that the dependencies between these areas are increasing and that their individual vulnerabilities thereby are increasing.

	Finance and Banking	Construction	Electricity	Fire and Rescue	Food Supply	Government (Management)	Industry	Media	Medical and Health	Military	Oil and Gas	Police	Telecommunication	Transportation	Water Supply	Workforce
Finance and Banking			x	x		x							x			
Construction	x		x			x	x				x		x	x		x
Electricity				x		x	x				x		x			x
Fire and Rescue		x	x			x						x	x		x	x
Food Supply	x		x			x	x						x	x		x
Government (Management)			x					x				x	x			x
Industry	x		x	x		x					x		x	x	x	x
Media			x				x						x			x
Medical and Health			x	x	x	x	x					x	x		x	x
Military			x		x	x	x				x		x		x	x
Oil and Gas	x	x	x	x		x	x						x	x		
Police			x			x							x			x
Telecommunication			x	x		x	x							x		x
Transportation		x	x	x		x	x				x	x	x			x
Water Supply			x			x	x						x			
Workforce	x		x		x	x		x	x				x	x	x	

Figure 5. Overview of the interdependence of important society areas[6]

[6] This matrix is an extended and updated version of a similar matrix published by The Norwegian Defence Research Establishment (1997).

3.2 GRID LAYERS

Looking at the vital infrastructures or businesses from a network centric perspective, three grid layers are apparent as illustrated in Figure 6. The upper layer can be considered to represent the businesses themselves and their interrelationship. It is referred to as the business grid. As we have already discussed, this is a layer with strong dependencies, and it can be seen as a strongly developed grid.

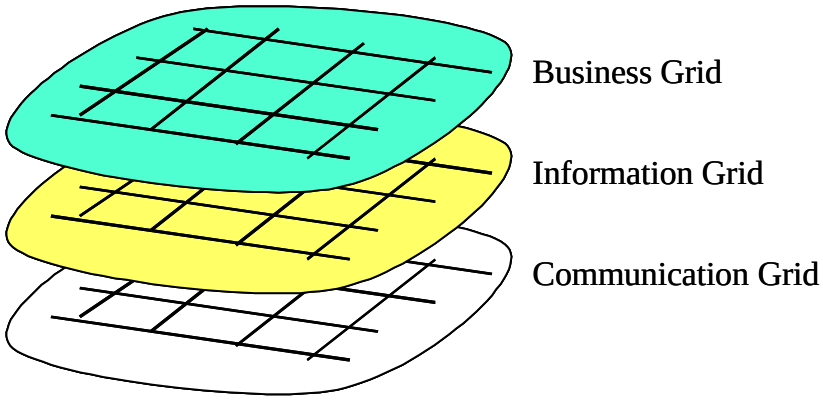


Figure 6. The three network centric infrastructure layers

The second layer is the information grid. This grid is not a technological grid. It is made up of the information and knowledge itself as required by the individual businesses. As of today, most public and private businesses keep this part to themselves. The lack of sufficiently secure mechanisms to share a lot of this information electronically has so far represented a major constraint. But even if this is solved, the information itself is not easily sharable. The way businesses structure and store their information is not standardised. So, even if it was freely available to a second party, it is not sure that the information needed could be found without guidance. This means that interfaces have to be prepared in advance, and tailored to a large extent to each and every joint venture. By interfaces in this context we mean policy (what to share), procedures (how and to whom), and at last the formatting of the information. This is to a large extent the way it has been so far. Severe crises, at least in a national or international context, creates to a certain extent chaos. We prepare ourselves in order to be able to handle such situations, but getting control will always require some ad hoc solutions. This adaptability and flexibility required in crises management is a quality that the information grid as of today is missing. So, the information grid is by far underdeveloped compared to the business grid it is supposed to be a part of.

The third and lower layer in our model is the communication grid. It is responsible for the transportation of the information between businesses as required. The communication grid is made up of a broad variety of communication means such as the postal service, telephone, Internet (World-Wide-Web) and even face-to-face communication. In our case, however, we will only consider Internet as a mean of sufficient availability and capacity to serve our businesses efficiently, when assuming that most of the information to be shared is stored on computers. There is no doubt that this is a strongly developed grid with the potential of connecting all business and individuals worldwide.

We therefore conclude that both the business grid and the communications grid are well developed, while the information grid represents the limitations in our ability in preventive and effective crisis management. When a crisis strikes, it will touch several elements within the business grid, while the information required to handle the crisis will reside in relatively inaccessible and different locations. The correlation and grouping of this fragmented and detached information is difficult and to a very limited degree made possible today.

3.3 A NETWORK CENTRIC SOLUTION

In order to improve our ability to manage crises, we need to come up with a concept that deals with the limitations of the information grid layer as described above. From a network point of view, this can be done in either of two ways. Our traditional approach would be to centralise management and information. A dedicated ministry, department, or government office is established to be responsible for national crises management. The other alternative could be the network centric solution, where the limitations inherent in today's information grid are overcome, and where information is dynamically made available across the businesses as required. This is illustrated in Figure 7.

The problem of centralisation is the inherent increased vulnerability. The information structure and the information carriers both become a critical vulnerability, and this is not acceptable. Therefore, a transition towards a network centric concept is most likely to happen.

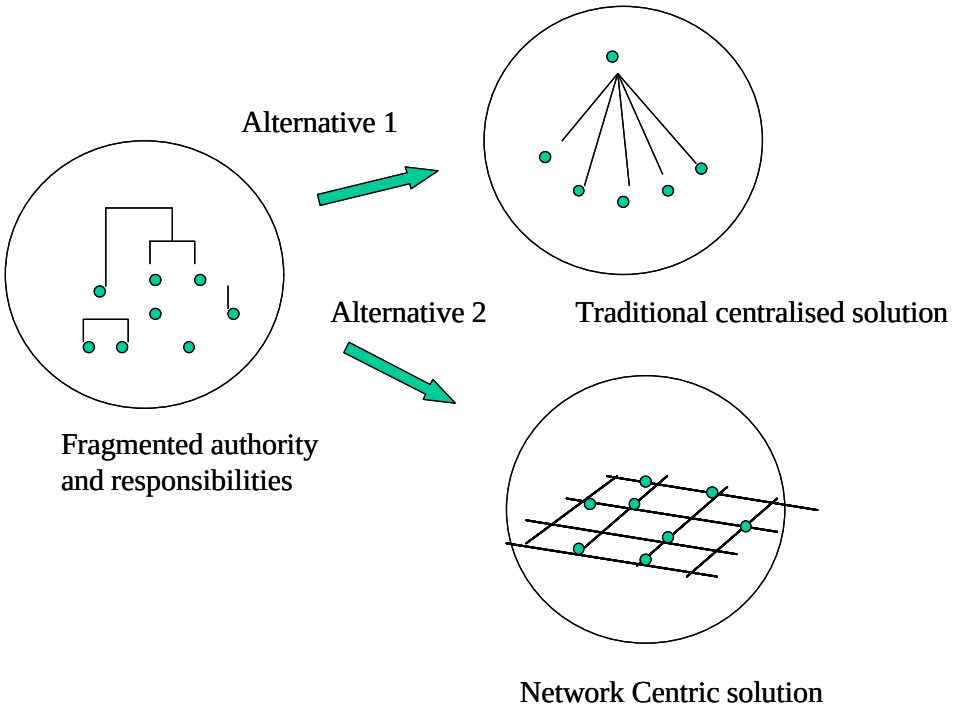


Figure 7. Alternative solution to centralized information management

4 SUMMARY AND CONCLUSIONS

This paper has brought forward a couple of examples illustrating the network centric nature of the vital business structures that make the modern society function. The underlying information structures, however, are still characterised by proprietary formats, organisation, usage and storage of information. As a consequence, bureaucratic procedures are used to regulate flow of information. This brings about a limited ability to handle crises in an effective manner.

Based upon these findings it is evident that a network centric crises management concept, where many of the limitations inherent in today's information grid are overcome is desirable. It is therefore predicted that a transition from today's trends towards more centralised concepts will gradually shift into a direction where a fully developed network centric crises management concept is the end state.