Network Centric Operations in Crisis Management

Josine van de Ven
TNO Defensie en Veiligheid
josine.vandeven@tno.nl

Richelle van Rijk
TNO Defensie en Veiligheid
richelle.vanrijk@tno.nl

Peter Essens
TNO Defensie en Veiligheid
peter.essens@tno.nl

Erik Frinking
The Hague Centre for Strategic Studies
erik.frinking@hcss.nl

ABSTRACT

This paper describes the approach to implement network centric operations (NCO) in the Dutch crisis management domain. NCO resolves a number of important shortcomings related to the supply and flow of information experienced in current verbal communication-based crisis management.

First, we provide a description of the crisis management organization in the Netherlands and the nature of information supply problems. Second, we explain how a network centric approach would be implemented in this domain. Next, we describe how between 2005 and 2008 several regions in the Netherlands have made efforts to implement a network-approach, and we evaluate their experiences.

The NCO approach reduces the need for reliability checks of verbal communication. Consequently procedures can be optimized with NCO. This paper concludes with next steps, such as continuing to explore the effects of NCO on the current way of working and train people to work in a network centric environment.

Keywords

Network centric operations, NEC, crisis management processes

INTRODUCTION

In the past eight years a number of critical incidents and crisis occurred, like in Madrid, 9/11, the Tsunami to name only a few of the most shocking crises world wide. In the Netherlands we had the Firework disaster in Enschede and fire in a cafe full with youngsters on New Year’s Eve in Volendam.

The scale, intensity and nature of incidents are increasing, as is the impact on society. To control the impact of these kinds of disasters it does not only take more resources, but also the number of organizations involved in a crisis response operation increases, e.g. the military forces, companies of critical infrastructures (e.g. electricity and water) to name a few. All these organizations have their own task and responsibility, which requests a new perspective on how to collaborate, share information and manage resources between the organizations. These needs must be addressed to increase professionalism of the crisis management organization.

The focus of this paper is on sharing information, especially sharing information between different units of the crisis management organization (e.g. police, medics, etc.). Although each has its own expertise and its own tasks during a crisis, the better they work together and share information the more effective is the crisis management. In our view sharing information is a good starting point to increase professionalism because it will support the collaboration between units which will increase shared situation awareness among the units. Although the type of information can range from plain facts to the decisions taken, for this paper we focus on exchange of factual information on the incident.

In this paper the term organization will be used to indicate the entire multidisciplinary crisis management organization, thus police, fire brigade, medic etc.. Each unit, e.g. the police, can be an organization itself, but will be referred to as a unit within the organization. The term team will be used to indicate a subgroup within a unit and a multidisciplinary-team consists of people from different units.

The Military started Network Centric Warfare (NCW) to share information across a network, because having a superior information position provides a lead in a battle with the opponent. However the concept is interesting for a broader audience, hence the term Network Centric Operations (NCO; Alberts, 2007) was introduced. NCO is an operational concept in which information is shared throughout the organization, vertical and horizontally. People needing information to take a decision or fulfill an assignment have access to the information, even when it is provided by a person from another unit. The NCO concept also supports mission planning together with other units, and at ultimo supports a self-synchronizing organization. Military organizations, like in the United States and the Netherlands, are already experimenting with this new way of working. The results of sharing information across a large organization with different units are positive on planning and decision making. Therefore it is interesting to find out if the crisis management organization can also benefit from the positive results of sharing information across an organization. In 2005 a field trial was set up in the Netherlands to use NCO in the crisis management organization, Defense cooperated in this. Following the positive results of this field trial, some case studies were set up and carried out in several regions in the Netherlands in 2006 and 2007. This paper describes the general results of these case studies where TNO was involved as expert-reviewer of the NCO-concept.

CRISIS MANAGEMENT IN THE NETHERLANDS

A crisis management organization in the Netherlands consists of multiple teams and multidisciplinary-teams acting at four different levels with different tasks and responsibilities (van Rijk, Post, and Verseveld, 2001). The four levels are the policy, operational, tactical, and field level. Depending on the severity of the disaster the Dutch crisis management organization can involve different organizations at different levels.

Hierarchical layers

The magnitude of the crisis management organization is based on the severity of the incident, which is indicated by GRIP-layers (Gecoördineerde Regionale Incidentenbestrijdings Procedure: coordinated regional incident-control procedure). There are five layers in total. The first one is ‘zero’ and indicates that the operational services are carrying out their normal activities. GRIP-1 is proclaimed for smaller incidents, where only the location of the source is involved. GRIP-2 is announced when not only the location of the source is involved but also an (small) effect area around it. GRIP-3 is proclaimed when the wellbeing of large groups of civilians are threatened. The last level, GRIP-4, is pronounced when the effect area of the incident crosses municipal borders and threatens neighboring towns. When a GRIP-4 accident occurs, the teams shown in Figure 1 will all be involved and include regional officials at the policy level. GRIP-3 also includes all levels, however the composition of the policy level differs from GRIP-4 in that local officials are involved. GRIP-2 includes the field level, tactical level and policy level, and in a situation called GRIP-1 the field-level and tactical level are involved.

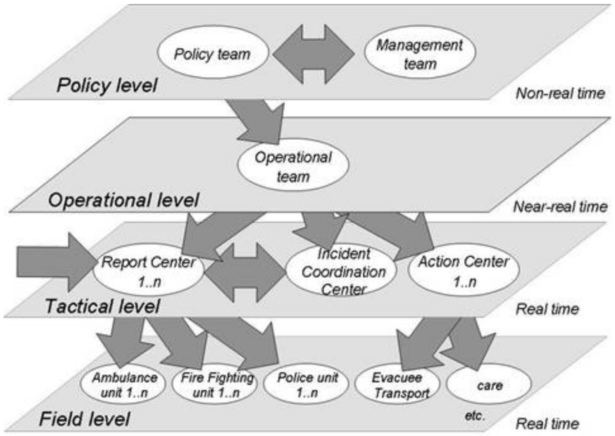


Figure 1. The levels in a Dutch crisis management organization.
Arrows indicate communication between teams. (Schaafstal et al., 2003)

Horizontal levels

The field level (see Figure 1) consists of teams operating at the incident place, e.g., police, medical personnel and firemen. These people act upon decisions made by higher-level teams. In addition, changing local information, which in a worst-case scenario could be the cry: “Run for your life!” has an immediate impact upon these units’ response.

At the tactical level (see Figure 1), the Incident Coordination Center (CoPI-team) coordinates all tasks carried out at the incident place. It gathers detailed information at the scene and continuously interprets the situation at hand. It is responsible for the implementation of actions decreed by the operational level and in turn provides the operational level with information from the incident place. It also immediately reacts to a changing environment. Action Centers coordinate activities away from the incident place, like registering and providing shelter for evacuees. All incoming emergency calls are received in the Report Center and are passed on to the Incident Coordination Center team or to relevant units. Different units (e.g. police, ambulance) usually have separate report centers, though this may vary, depending on the region. In the future, most Report Centers will be combined.

Those working at the operational level (see Figure 1) are responsible for the coordination of various processes. They generate input for policy-making at the highest level, act upon decisions made by the policy level and are responsible for the execution of these decisions. They gather and combine information about the situation at hand from the tactical level and pass it on to the policy level. The operational team does not operate at the incident place and does therefore not receive first-hand information.

High-level organizational matters (e.g. those concerning multiple regions) and legal matters are discussed at the policy level (see Figure 1), with the mayor as head of the policy team. They make the larger-scale decisions, such as to evacuate an area or to ask for support from other regions, taking into account both information from the situation at hand and the implications of their decisions. Decisions made by the policy team are passed on to the tactical level, where they are converted into more detailed plans and put into action.

More governmental organizations are involved when disasters become over-regional and may have an effect on the entire country, like a terrorist attack or bird flu, or may take several days or involve scarce resources. Figure 2 shows the entire crisis management organization for large incidents. The structure is being build during a crisis when it is realized how large the impact really is. It usually starts with the field units, and then adds the tactical level and operational level, up to the policy level.

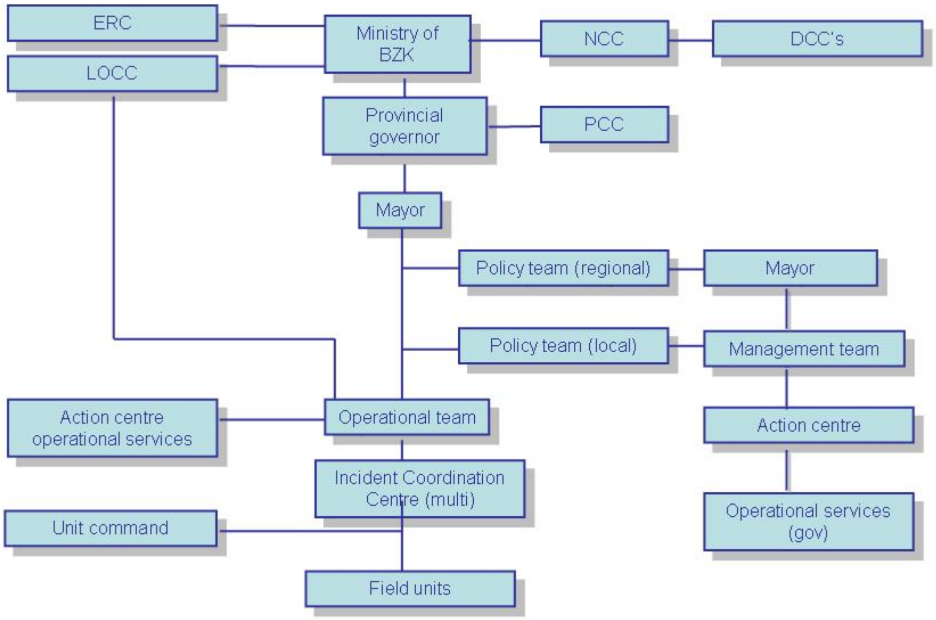


Figure 2. Entire Dutch crisis management organization, including ministerial involvement (The Ministry of the Interior and Kingdom Relations)

ERC = Expertise Centre for Risk and Crisis Communication
LOCC = National Coordination Centre for operational services
NCC = National Coordination Centre
PCC = provincial Coordination Centre
DCC = ministerial Coordination Centre
BZK = Ministry of the Interior and Kingdom Relations

Limited Situation Awareness in the Traditional Approach

By the time the higher levels become active they are informed of the incident by several units, all stove-pipe organized. All this time new people need to get familiar with the incident and require information that is available at the lower levels. Informing teams at different levels of the stove pipe is done using situation reports. When these situation reports would not be send, the only other way to be kept informed is to call ‘friends’ at other levels, creating a communication overload. Situation reports are very useful to inform other units and teams of the situation on the incident location (by tactical team) and the effect areas (by operational team), but there are some drawbacks. The three main drawbacks are:

1. it takes time for a situation report to arrive at the other teams especially those higher up in the structure;
2. situation reports provide a static view of the situation and are out-dated the time they are send out;
3. not everybody who needs the information has access to these situation reports.

Thus the situation awareness within the organization is limited because by the time information has reached its destination it may be outdated.

Before discussing the effects of network centric operations on these issues however, it is useful to present the foundations of network centric operations a little more than we did thus far and describe the steps used in the Netherlands for the network centric experiment.

NETWORK CENTRIC OPERATIONS

Network Centric Approach

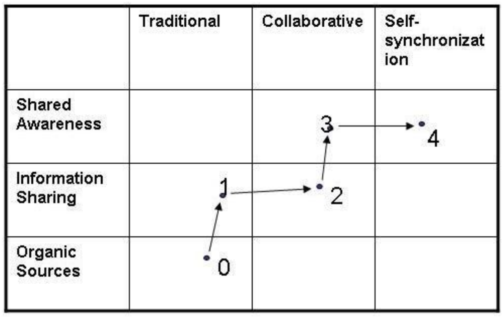
Already in the previous century it was recognized that to improve decision making one needs to have a better situation awareness of the situation which is achieved by knowing more about it (Alberts, 2007). Usually there are two main limitations to this, time and information. We have to deal with time limits and the fact that we have not all the information on the situation when we have to decide. Network Centric Operations is a way to improve sharing information in complex situations, where multiple units are involved. However network centric operations is more than just information sharing.

According to Alberts (2007) there are four domains that describe a network-centric organization:

1. Physical domain: All units of the organization (Alberts calls this an enterprise, in this paper we will continue to use the term organization) are robustly networked and should support connectivity and interoperability between all.
2. Information domain: All individuals in teams have the capabilities to share and access information within the organization.
3. Cognitive domain: All individuals in teams have the capabilities to develop high quality awareness.
4. Social domain: The individuals in teams are capable of self-synchronization, by developing shared awareness and understanding.

Having a robust network to share information better, shared awareness will result in improved decision making and enable self-synchronization. In complex situations where an incident is controlled by many teams, as a crisis usually is, each team has it own goals. The fire department puts out the fire, the police take care that the location is controlled and everyone gets out, or in if needed, and the medics treat the wounded. So there are three teams with three individual plans to fight the crisis. However to control complex situations having three individual plans is not effective because the effects of an action are unknown but above all very important to all. To increase the effectiveness of plans to control the situation and make use of all capabilities available, teams need to synchronize their plans. Thus self-synchronization is important in network centric operations because it will lead to improved use of capabilities to control the situation. Self-synchronization requires a level of shared awareness, this means cross-domain awareness as well as awareness across domains. To build up shared awareness all teams need to share information and share understanding of the situation. (Albert, 2007)

Organizations should strive to implement self-synchronization to get all the benefits from NCO. Alberts suggest a maturity model to go from the traditional command and control process (level 0) to self-synchronization (level 4), see Figure 3.



	Traditional	Collaborative	Self-synchronization
Shared Awareness		3	4
Information Sharing	1	2	
Organic Sources	0		

Level 0: baseline, traditional command and control
Level 1: significant amount of information sharing
Level 2: collaboration across location, function and organization among participants
Level 3: Improved level 2, by not focusing on sharing information but on what it means
Level 4: permits self-synchronization

Figure 3. Network-Centric Maturity Model (Alberts, 2007)

Alberts describes the steps and provides information on knowledge already available. How far* an organization will actually go in implementing network centric operations and how that is done, is not so easy to describe. In the previous paragraph we wrote something about the traditional way of working in the Netherlands, the next will provide more information what was done to go from level 0 to level 1 in the above mentioned maturity model.

Development in crisis management

The aim of the field trial in 2005 was to establish whether the NCO Command and Control concept of the defense organization at level 1 of the above mentioned maturity model is also applicable in the crisis management domain. The research objective was to determine whether the network centric approach contributes to an improved information distribution for all the participants in a crisis management organization. Three regions and the defense organization, LOCC and NCC participated in this field trial. Based on the results of this trial it was concluded that the network centric approach certainly has advantages for the emergency management domain, especially for the distribution of information. A necessity is that the available technique (hard- and software) is functioning properly, which is the goal of level 1 in the maturity model (Figure 3).

The field trial was held in three regions involved (of the 25 in total). The success of this trial let to the case studies in 2006 and 2007 where more regions of the Netherlands were involved. During the case studies the concept of the network centric approach was distributed across the Netherlands on a voluntary base for those regions that participated. The case studies focused on providing a better network, improved exchange of information and improved situation awareness. The Ministry of the Interior and Kingdom Relations (BZK) initiated the case studies and provided the project manager, but several more organizations were involved in carrying out the project, a few are mentioned hereafter. The Dutch Defense organization was involved because of their knowledge of network centric operations and their experience with the technical issues. M&I partners were involved because of their expertise in information management and change-management. TNO was involved because of the expertise of NCO and performed observations during the cases studies.

To make the transformation from the current way of working to a network centric way of working, a two-way approach was taken. First, throughout the year workshops were held (Ministerie van Binnenlandse Zaken, 2007) introducing and discussing network centric operations with people from crisis management organizations within the country. Second a software application that resembled an application already used in some regions was introduced and used. These applications combined a textual form, for incident data and situation reports, with a graphical map. This allowed participants to build up their situation awareness using both textual and graphical information about the crisis during the case studies.

EVALUATING EFFECTS OF NCO

The case studies were set up in a practical way and usually coincided with the normal training of that particular region. Therefore every study was unique, and not standardized. In some regions only the tactical level (see Figure 1) participated in the training, while in other regions the tactical and operational level participated. One large training was held in 2007 which included LOCC and NCC for the observations next to the tactical and operational level (see Figure 2). In total five cases were observed in different regions of the country.

Observation Framework

We first developed a framework to report the observations in a standardized way. This was necessary because all case studies were unique, in e.g. units participating and scenario. This way results could be compared with each other to see if similar results were found in different regions and different teams. The framework has three main factors:

1. Technical and organizational aspects during the experiment; the main question to be answered here is how accessible is information for participants? Can they access information within their unit and the organization?

* In principle going up to level four is network centric operations, beyond that it is only partially implemented.

2. Actual information available; the most important question here is whether all information of the incident is made available during the experiment (like: GRIP-level, resources available, etc.). Which information could have been available is directed by the script of the exercise.
3. Situation awareness; What is the 'Situation Awareness' (SA) of the participants. The model of Endsley (2003; see Figure 4) is used to differentiate between the three levels of SA: 1). Perception of data and the elements of the environment, 2). Comprehension of the meaning and significance of the situation, and 3). Projection of future states and events.

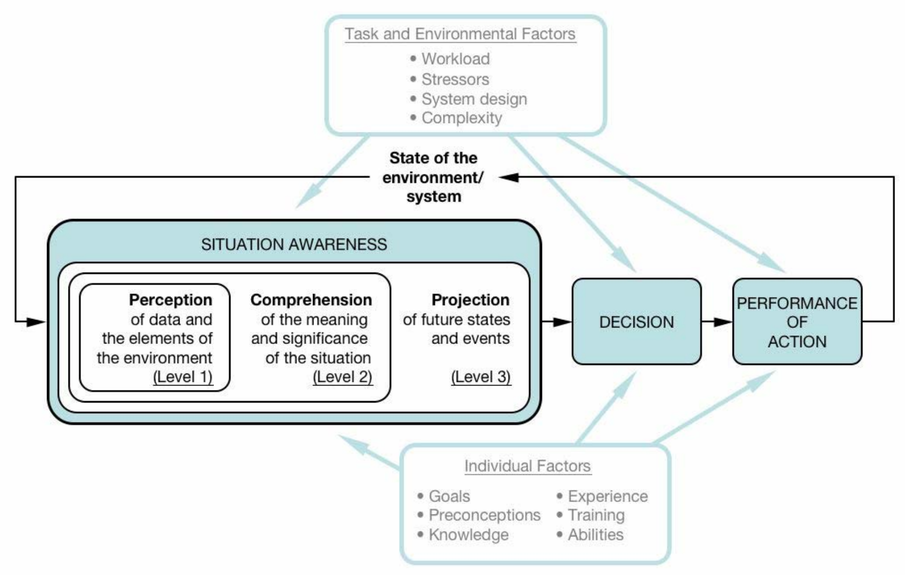

Task and Environmental Factors
• Workload
• Stressors
• System design
• Complexity
State of the environment/ system
SITUATION AWARENESS
Perception of data and the elements of the environment (Level 1)
Comprehension of the meaning and significance of the situation (Level 2)
Projection of future states and events (Level 3)
DECISION
PERFORMANCE OF ACTION
Individual Factors
• Goals
• Preconceptions
• Knowledge
• Experience
• Training
• Abilities

Figure 4. Endsley's model on situation awareness (Endsley, Bolté en Jones, 2003).

Data collection

Making observations during the case-studies was a challenge. We were restricted during the observations because we were not allowed to make audio (or video) recordings during the training. In some situations we were not able to be in the same room as the team under observation and we used monitors to follow the meeting and perform our observations. Only in one situation we were granted access to the logged data from the system.

During the exercises we observed a team during their multidisciplinary meetings and wrote down the conversations. We wrote down the subject and how it was uttered (e.g. stated as facts, questions, etc.). Other related meta-data recorded was the person speaking (role), the time and the addressee (when a particular person was addressed). When possible we also tracked information exchange outside the multidisciplinary meetings, these were usually mono-disciplinary (telephone) meetings or bilateral meetings between for example fire brigade and police. When possible we held interviews after the exercise with some of the key players in the scenario, usually the leader of the team and/or the person responsible for the information processing in the system. The recorded data was clustered into the three factors of the framework. We discussed our observations (about what we had seen and in which context) with TNO NCO-specialists to summarize the data.

Results

Using the framework described in the previous paragraph all cases were evaluated. In this paragraph the results are combined into one general view on the effects of network centric operations for crisis management in the Netherlands. The most important results are listed here, all of them were collected in more than one exercise. We believe that they can be used as a starting point for transformation to the second level of the maturity model (see figure 3). However the transition to level two will incorporate more than only these issues mentioned in the next paragraphs.

Technical and organizational aspects

- *Create access at all levels to the information*. In principle all data (text and graphics) is available for every person in the organization as long as they have access to the application, given their access rights. At this moment application access is easier higher up in the hierarchy, because of easy access to computers. At the CoPI-team and field level (see Figure 1) access is limited, because of the limited access to computer-technology. The information manager of the CoPI-team has access to the system, this person enters information from the CoPI-team (and field units) into the system and reads the information from the other teams and distributes this amongst the CoPI-team. Others in the Copi-Team and field units receive their information via telephone or '*two-way radios'* both are easier to access in the field. Whether in the future field units will have direct access to the information system remains to be seen, as their primal focus is fighting the incident. However it is vital for the shared awareness that these people also have access to the information, either by having access to the system itself, or by having a contact person that has access.
- *Encourage professionalism in an information rich environment*. The network centric way of working indicates that information is available for all. At first people at all levels complained about this, because it allows others to 'poke' around and mind others people's business. Thus network centric operations request a professional approach from crisis management organizations. With regards to this point it is also important to provide people with the correct information needed for their task.
- *Provide different information formats for different needs.* A last point we would like to mention here is that although all levels have a need for both textual and geographical information, the importance for either form is different at the different levels. For example the geographical data shows the current situation and is therefore of more importance to the teams lower in the organization.

Actual information available

- *Learn to be aware of, and deal with, possible conflicting information*. Although to deal with conflicting information was always an issue, the network centric approach makes possible conflicts in information stand out clearer because information is accessible for all. During the observations we knew that people had other information than available in the system. For several reasons they did not share this with the others and started to doubt their own information. This happened especially with information that is not directly related to a person's own task. For example a police officer that had information on wounded people in a specific area that did not corroborate information given by de medics, did not put this number in the system or in any other way contacted (immediately) his colleague in the medic department to discus the information. After the debriefing both the police officer and the medic felt that it would be better to discuss this fact in the future as it could help both.
- *Create awareness that information might be interesting for others, and train on formulating information*. At this moment people enter information in the system that they find interesting themselves, and use jargon to formulate it. This makes it harder for others to understand the message and because not all information is added others might not be able to find what they need. This shows a large difference between the current way of working and the network centric approach. The current way is much more focused on the teams individual task and goals, whereas network centric is much more focused on the multidisciplinary way of working.

Situation awareness

- *Differentiate between facts and assumptions.* Information is shared between the different teams in the organization to build a shared situational awareness. Information can be qualified as facts or assumptions. During the study we heard people stating assumptions as facts and hardly ever as assumptions, thereby (unintentionally) misleading others. It is important to be explicit what kind of information is used. Ideally only facts are communicated between the teams to prevent decisions being based on fault assumptions. However sometimes it is useful to report assumptions, but they must be identifiable to prevent miscommunication and incorrect decisions.

- *Each team in the organization has its own tasks and responsibilities for which the available information is used.* Each team builds its own situation awareness, for their own task, based upon the information available in the system. The information of other teams is used as input but needs to be processed before it can be implemented. Therefore the different teams have different needs, although everything is about the same incident. The CoPI-team usually inputs the main part of the information on the incident, as they are at the location itself. The CoPI-team that is coordinating the fighting of the crisis is mostly working with facts (the fire is located at building A) and assumptions (the gas that is spreading is toxic gas *X*). Their situation awareness based on this information might be that they need protective clothing for the firefighters and need a specific substance other than water to extinguish the fire. The operational team focus on the area around it and use the same information to build up their situation awareness. Their situation awareness might be that the toxic gas is endangering area W, and that they need to move people out of that area.
- *The information system can function as a pre-warning system for teams higher-up in the hierarchy.* The moment an incident starts not all teams in the crisis management organization are active. Teams higher in the hierarchy are alerted later on if an incident is scaled up. These teams lose extra time to collect information needed to build awareness of the situation. If they have access to an information system in which all relevant information is available, they can reduce the time needed to become aware of the situation and start immediately managing work to be done at their level.

The above observations show that most of them are related to benefit from the network and learn to work with it, thus to collaborate with others in the organization. This shows that the transformation from level one of the maturity model (Alberts, 2007) to the next level will not happen on its own accord.

CONCLUSION AND DISCUSSION

The case studies that were carried out these last two years have provided the opportunity to get acquainted with NCO within the crisis management domain. The results of the trial in 2005 show that what was originally a initiative in the Military domain, to improve decision making and planning of complex endeavors, also works to fight crises. The observations of the case studies indicate that the Dutch approach is currently at maturity level 1 (Alberts, 2007). To move on to level 2 of the maturity model the next steps need not only focus on the technical capabilities, but should also focus on training individuals in the organization and research the effects on the operating procedures. This is not that easy because of legal issues involved in the crisis management domain, that for example dictate the structure of the crisis management organization. However within the legal boundaries there is still enough space to experiment with the NCO-way of working. On the training part we see a shift from the actual fighting of the crisis to learning to operate in a network centric approach. People have to learn the basics of network centric operations (e.g. share information, find information) in order to be able to act in an network centric way. Besides that they have to develop their individual network centric capabilities, e.g. the cognitive and social domains of fundamental capabilities. In moving up to the next level of the maturity model, there will be some effects on the information needs (information domain) which will reflect in additional requirements for the information system, which means that the system needs to be developed during the implementation of the NCO approach. We have seen that NCO improves the information process and supports a shared awareness of the situation. The real benefit of NCO will be realized only if training of people in working in an network is implemented

ACKNOWLEDGMENTS

We would like to emphasis that many people, from different organizations, participated in the work described in this paper. We would like to acknowledge their contribution to our work, without their hard work our observations would not have been possible.

Special thanks to the regions involved in the case studies: Veiligheidsregio Noord- en Oost Gelderland, Regio IJssel-Vecht, Hulpverlening Gelderland-Midden, and Veiligheidsregio Rotterdam Rijnmond were we participated several times.

REFERENCES

1. Alberts, David S., and Hayes Richard E. (2007). Planning: complex endeavors. DoD Command and Control Research Program, Washington, DC, available at: www.dodccrp.org.
2. Endsley, M. R., Bolte, B., & Jones, D. G. (2003). Designing for situation awareness: An approach to user-centered design. Taylor & Francis. London
3. Ministerie van Binnenlandse Zaken, and Ministerie van Defensie [The Ministry of the Interior and Kingdom Relations and the Ministery of defense] (2007). Effectievere besluitvorming bij rampen, crises,calamiteiten en incidenten [effective decision making with disasters, crises, and incidents].
4. Van Rijk, R. Post, W.M., and van Verseveld, O.H. (2001). CrisisKit: Ontwikkeling en evaluatie van een omgeving voor samenwerkingsprocessen bij rampenbestrijding. [Crisiskit: Development and evaluation of a program on team processes in crisis management]. (Rep. No. TNO-TM-01-D016). Soesterberg: TNO Defense, Safety and Security.
5. Schaafstal, A.M., and Post, W.M. (2003). Oefening “Duikeling”: BT/OT te Diemen op 12 september 2002. [training Duikleing Policy level and Operational level in Diemen (near Amsterdam in the Netherlands) on September 12, 2002] (Rep. No. TNO-TM-03-C004). Soesterberg: TNO Defensie en Veiligheid.
6. Veiligheidskoepel (2006). Referentiekader GRIP. http://www.minbzk.nl/onderwerpen/veiligheid/crisisbeheersing/publicaties?popup=true&ActItmIdt=99130