Organizing Emergent Safety Organizations

The travelling of the concept 'Netcentric Work' in the Dutch Safety sector

Kees Boersma
Faculty of Social Sciences
VU University Amsterdam
Fk.boersma@fsw.vu.nl

Jeroen Wolbers
Faculty of Social Sciences
VU University Amsterdam
J.Wolbers@fsw.vu.nl

Pieter Wagenaar
Faculty of Social Sciences
VU University Amsterdam
FP.Wagenaar@fsw.vu.nl

In: *Proceedings of the 7th International Conference on Information Systems for Crisis Response and Management ISCRAM.* Seattle, April 2010. S. French, B. Tomaszewski and C. Zobel (eds.): 1-6.

INTRODUCTION

> 'The social networking site Twitter again stole a march on traditional media when it was the first outlet to publish dramatic pictures of the Turkish Airline crash. Moments after the plane crashed at Amsterdam's Schiphol Airport on Wednesday morning the news was appearing on Twitter… This proves that social networking sites can be a real asset in covering breaking news and gathering eyewitness accounts but the web should always be treated with extreme caution.' (CNN, 2009).

Moments before the crash, at 10:31 in the morning, one of the Schiphol air traffic controllers contacted the Emergency Response Room (ERR) of Kennemerland (the safety region which Schiphol is part of) in Haarlem (a city close to Amsterdam) because the plane was missing on the radar. It was, however, the social networking sites that delivered the most adequate news to the public. Civilian journalism – that is citizens spreading the news - had put its stamp on the discussion about emergency management. Shortly after the first call emergency response teams were leaving the fire stations, hospitals and police stations. Notwithstanding the relatively quick response almost immediately discussions arose about the (quality of) information available for the first responders, the responsible commanders and – most important – the policy-makers (of the region).

The above event has caused many (political) discussion in the Netherlands. This discussion is part of a longstanding debate about the organization of the civil safety sector (see also: Boersma et al., 2009). The most recent development in the field, and central to this article, is the introduction of 'netcentric' work. It has been introduced in the field of emergency and crisis management to improve the exchange of information between heterogeneous actors involved in crisis and emergency management. Netcentric work is meant to overcome the difficulties in information sharing practices. Besides, netcentric work can be seen as an attempt to close the gap between '(…) social demands for control and security, and the capacity for systems of rational management and administration to satisfy these demands' (Power et al., 2009). The idea is that netcentric work can break through

the established patterns of command and control. In a way, netcentric work is supposed to enable networks of communication within a bureaucratic environment – the direction is not per se towards a network organization.

The question is, how, in the Dutch situation, the ministry of Home Affairs is trying to force one (technical) standard for netcentric work while at the same time giving room for local inventions in the various safety regions. Next, once in use in the safety regions, netcentric work follows the principle of soft-bureaucracies (Corpasson, 2000). That means that at times of crisis it is the bureaucratic organization that will provide standardized organizational principles for emergency response leaving it at the same time to the local professionals *how* these principles are executed. The main question in this working paper is what determines the choices made by the various safety regions (how) to translate and implement the netcentric principle, if at all?

Concepts of Netcentric Work

Netcentric work means that the emergency response professionals together with administrators (e.g. representatives of the municipality) not only collect real-time information about a certain incident but are able to create what is called a *common operational picture* (Mendonca et al., 2007; Moynihan, 2009). The common operational picture means that every 'authorized person' has access to the information regarding an incident that has been put on a web-based platform.

Creating a common operational picture is considered to be important, since any analysis of decision-making processes during incidents makes clear that remote and just-in-time information and expertise is crucial for an adequate emergency response. That is not to say that all the information possible at the time of an incident should be available for everyone in the field – local response personnel should not be constrained by formal information structures that will prevent them for improvisation and for being creative (Mendonça et al, 2007). The idea, however, is that the common operational picture facilitates an optimal situational awareness for all professionals – this is just one, but not *the* precondition for emergency response. Netcentric work, in technical terms, is based on the idea of network-enabled capability (NEC), which '(…) constitutes an enabler of effects-based operations both at the level of command and control, and at the level of operational capability.' (Von Lubitz et al., 2008: 10).

NETCENTRIC WORK IN ACTION

What is anticipated on with the introduction of NEC is not so much an implementation of a new technical device but, as one of our respondents at the Dutch Ministry of Domestic Affairs told us, a *paradigm shift* and a new way of information sharing, working, and organizing. Considering netcentric work more closely and in context, it is not easy to define its consequences for the bureaucratic organization. Since it has been introduced as a paradigm shift, it can, however, be seen as a reaction to the bureaucratic, Weberian way of organizing the civil safety sector, in which organizations are centrally governed, and the power is delegated on the bases of obedience. When we consider the impact of network enabling technologies in-use one can question whether Weber's model is still an adequate description of domination and legitimation.

Questioning the public sector is not new - it has been debated since the 1980s, a decade in which political leaders implemented New Public Management (NPM) doctrines (Osborne and Gaebler, 1992). NPM

rejects Webers idea that government is best served by bureaucratic organizations i.e. by domination and obedience. With its emphasis on public-private partnerships and privatisation of governmental bodies, however, NPM does not fully reflect the situation in the Dutch safety sector. Although typical NPM characteristics such as the introduction of performance indicators have affected the sector, it is not so much the public-private partnership that is at the heart of the discussion.

The debate, really, is about steering of networks of heterogeneous actors who still fall under the responsibility and structures of domination of government. Instead of implementing NPM strategies, the Dutch safety sector has implemented decentralization in combination with further centralization. A strict centralization in the sector can count on strong opposition because it presupposes a monolithic and strong official culture based on solidarity (Jermier et al., 1991). However, the various sub-cultures of the 25 Dutch safety regions and the subcultures of the disciplines (police, fire brigade and medical services) make it difficult, not to say impossible, to implement one formal netcentric principle including the technical tool. The development in the Dutch safety sector and the way it incorporates ideas of netcentric work can best be described with the ideas of soft bureaucracy, which… '… express the emergence of a political centralization of organizations, in line with the development of decentralized ways of conducting their activities: jobs and responsibilities have become more decentralized, but political decisions more centralized.' (Courpasson, 2000, cit. p. 155).

NETCENTRIC WORK IN THE NETHERLANDS

The start of a journey: NEC in the military

The idea of Network Enabled Capabilities originated in the military in response to the intensified collaboration between the three military branches (army, navy, airforce). Together with the idea of Netcentric Warfare, NEC emerged as the 'new way of working' in the military. NEC would 'transform the way in which armed forces operate' (Houghton et al., 2006, p.199) From interviews with advisors from the Ministry of Internal Affairs, who mostly had a previous career in the military, the importance of the project emerged: 'NEC implies a totally different way of thinking, that lesson is learned from the military'.

In the literature the terms Network Enabled Capabilities and Netcentric Warfare (NCW) overlap. Although very similar, NCW goes one step further than NEC. While NEC enables networked command and control, NCW uses networks as a doctrine. Network-centric warfare is the conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commanders intent, independent of the geographic or organizational disposition of the individual elements (…) (Fewell and Hazen, 2003, p.2). Perry et al. (2002, p.2) write that NCW is: 'the linking of platforms into one shared-awareness network in order to obtain information superiority, get inside the opponents decision cycle, and end conflict quickly'. The four tenets of NCW are (Albers et al., 2000):

- A robustly networked force improves information sharing,
- Information sharing and collaboration enhance the quality of information and shared situational awareness,
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command,
- These, in turn, dramatically increase mission effectiveness.

En route: from the military to the emergency response domain

The idea of NEC travelled from the Department of Defence to the emergency response domain through intensified civil-military collaboration (Home Office, 2006). The military assistance to the emergency sector is arranged in article 18 of the law on disasters and severe accidents, but has always limited itself to direct assistance, mostly in the case of flooding.

The Dutch parliament announced that the tasks of the Department of Defence must change from being a provider of direct assistance only to becoming a structural emergency partner and exchange resources and knowledge (Home Office, 2006). This included the exchange of resources from the military to develop the quality of the emergency response domain. In the Netherlands the software package ISIS (Integrated Staff Information System) was used as a NEC tool to comprise a battlefield image anywhere on the world. This system was used to monitor classified military operations in Afghanistan and Iraq from the Netherlands, one of our interviewees told us. It enabled the commanders to see the operational picture of the field.

The experience with ISIS leads to the use of this system in intensified civil-military collaboration. This was the start of several NEC experiments between MoD, Home Office and three safety regions. As one of our interviewees says: 'the technology was available from the Military, which meant that the technology only had to be adapted. Also a stable infrastructure was already present. It was no technology push from the defence department, but a good collaboration between the available technology from the military and the civil demands'.

The first range of NEC experiments started in 2006 and was used to align the military system ISIS and the Home Office system Incident master. Tested was if the several ICT environments could be integrated to achieve communication between the military and the safety regions.

The second round of experiments was arranged by the private research bureau TNO and involved nine of the 25 Dutch safety regions (including Rotterdam-Rijnmond, Haaglanden, Hollands-Midden, Zuid-Holland-Zuid and Utrecht). Tested was what happened if the incident information was shared between the emergency domain's disciplines. Important in this second stage was that the NEC tests were integrated into existing regional disaster exercises. Here the regions could test with NEC in operational context and fully experience the impact of Netcentric working. The region of Rotterdam eventually confronted NEC with the traditional way of working in parallel tests and concluded that NEC had major advantages.

Local adaptation

If we look at the way the regions have adopted netcentric work, we find we can plot them on a continuum, ranging from pioneering regions to regions that haven't adopted the concept at all. Gelderland-Midden, Brabant-Noord and Limburg-Noord are pioneers. Gelderland-Midden happened to have a project with a large software company and later learned that the project its local entrepreneurs had been working on was something elsewhere known as netcentric work. Brabant-Noord has a large air show in its region, which necessitated cooperation with the airforce and thus caused a very early transfer of netcentric work from the military to the civilian world, and Limburg-Noord belongs to a cluster of border regions, that has consciously developed its own netcentric work platform, because it needs to be able to cooperate with emergency workers across the border. Rotterdam and Leiden are both early adapters, although in a different way. Leiden concentrates on work-processes, whereas in

Rotterdam technology comes first. Haarlem is a competent follower. It waits for the Home Office to come up with netcentric work, and then adopts it. Dordrecht and Amsterdam still keep clear away from netcentric work because of other priorities. Yet there are similarities between regions as well.

CONCLUSION

Netcentric work is reinterpreted and redefined constantly as it travels through the safety sector in The Netherlands. It's not only the definitions, the goals, and the way of implementation of netcentric work that are constantly redefined; the technology turns out to be just as malleable. One of the reasons behind this constant (re)interpretation is that netcentric work travels in all directions. It is not only a top-down phenomenon that moves from the Home Office to the highly fragmented world of the Dutch safety regions, but also something such regions come up with themselves, borrow from the ministry of defence on their own account, or copy from other regions. The drivers behind netcentric work are the Home Office, the Ministry of Defence, technology itself - which emergency response workers already use in their private life - and a number of local entrepreneurs in the safety regions, all bringing their own agenda's, views on emergency response work, work routines, etc., which accounts for the wildly differing views on what netcentric work is.

REFERENCES

Albers, D.S., J.J. Garstka and F.P. Stein (2000). Network Centric Warfare: developing and leveraging information superiority, *DoDC4ISR Research Program*, Library of Congress.

Boersma, F.K., P. Groenewegen and P. Wagenaar (2009). Red, white and blue with a little bit of green: an ethnographic study into the Emergency Response Rooms in the City of Amsterdam. *Proceedings of the 6th International Conference on Information Systems for Crisis Response and Management ISCRAM*.

Courpasson, D (2000). Managerial Strategies of Domination. Power in Soft Bureaucracies". *Organization Studies*, 21(1): 141-161

Fewell, M.P and M.G. Hazen (2003). *Netcentric Warfare, its nature and its modeling*, Department of Defence Australia, DSTO Systems Sciences Laboratory.

Houghton, R.J., C. Baber, M. Cowton, G.H. Walker and N.A. Stanton (2008). WESTT (workload, error, situational awareness, time and teamwork): an analytical prototyping system for command and control, *Cognition, Technology and Work*, 10: 199-207.

Home Office (2006) Report Intensifying Civil-Military Collaboration, letter to parliament, 2006-0000175447

Jermier, J.M., J.W. Slocum, L.W. Fry and J. Gaines (1991). Organizational subcultures in a soft bureaucracy: resistance behind the myth and façade of an official culture, *Organization science*, 2(2): 170-194.

Mendonça, D., T. Jefferson and J. Harrald (2007). Collaborative adhocracies *and Mix-and Match Technologies* in Emergency Management, *Communications of the ACM*, 50(3): 45-49.

Moynihan, D.P. (2009). The network governance of crisis response: case studies of incident command systems, *Journal of Public Administration Research Theory*, Advance Access published on January 30, 2009. doi:10.1093/jopart/mun033.

Osborne, D. and T. Gaebler (1992). *Reinventing Government. How the Entrepreneurial Spirit Is Transforming the Public Sector*. Reading, MA: Addison-Wesley.

Perry, W., R.W. Button, J. Bracken, T. Sullivan and J. Mitchell (2002). Measures of effectiveness for the information-age navy: the effects of network-centric operations on combat outcomes, *Report MR-1449-NAVY of the RAND Corporation*.

Power, M., T. Scheytt, K. Soin and K. Sahlin (2009). Reputational Risk as Logic of Organizing in Late Modernity. *Organization Studies*, 30(2/3): 301-324.

Von Lubitz, D.K.J.E., J.E. Beakley and F. Patricelli (2008). Disaster Management: The Structure, Function, and Significance of Network-Centric Operations, *Journal of Homeland Security and Emergency Management*, 5(2), article 42:1-24.