# A Decade of Netcentric Crisis Management: Challenges and Future Development

**Jeroen Wolbers, Willem Treurniet, and F. Kees Boersma**

**Abstract** Information exchange is regarded as a vital component of crisis management, yet organizations continue to struggle with the timely distribution of information across organizational and professional boundaries in a crisis. In this chapter, we reflect on the doctrine of "netcentric operations" in the Netherlands, which has been implemented to enhance the quality and speed of information exchange in distributed crisis management networks. First, we provide an overview of the principal tenets of netcentric operations: self-synchronization, distributed sensemaking, information superiority, transparency, and connectivity. Next, we highlight five key challenges from a decade of operations: (1) how to codify and make sense of information; (2) how to foster goal-directed collaboration; (3) how to enable collaborative decision-making; (4) how to overcome a reluctance to share information; and (5) how to maintain functionality in extensive distributed networks. Finally, we specify future directions to improve connectivity and transparency and reflect on finding an alternative for self-synchronization.

**Keywords** Crisis management · Information management · Netcentric operations · Command and control · Networks

J. Wolbers
Leiden University, Leiden, Netherlands
e-mail: j.j.wolbers@fgga.leidenuniv.nl

W. Treurniet
Netherlands Institute for Public Safety, Arnhem, Netherlands
e-mail: willem.treurniet@nipv.nl

F. K. Boersma (✉)
Vrije Universiteit Amsterdam, Amsterdam, Netherlands
e-mail: f.k.boersma@vu.nl

H. J. Scholl et al. (eds.), *Disaster Management and Information Technology*,
Public Administration and Information Technology 40,
https://doi.org/10.1007/978-3-031-20939-0_5

## Introduction

In the past decade, information management is progressively recognized as a cornerstone of effective crisis management (Palen et al., 2007; Reuter & Kaufhold, 2018; Comfort, 2007). In rapidly changing and complex crises that bring forward uncertainty and equivocality, the quest for producing a shared overview through a common operational picture is of primary concern for crisis managers (Wolbers & Boersma, 2013; Boersma & Wolbers, 2021). The challenge of organizing a coherent crisis response requires both situational awareness and collaboration awareness, as a broad range of actors collaborate in multi-organizational networks (Treurniet et al., 2012). In the response network, each organization has different responsibilities and goals, which generates different jurisdictional and functional boundaries (Comfort & Kapucu, 2006). To overcome these boundaries, different systems are developed to enhance the quality of information sharing between response organizations.

A key doctrine that is being implemented worldwide is netcentric operations. It is envisioned that netcentric operations will enable a shared understanding of a crisis situation by linking individuals and their distributed networks through a shared information platform that allows the rapid and timely sharing of information, which in turn leads to better, more informed decisions (Houghton et al., 2008). Yet, the past decade has shown that improving collaboration according to netcentric principles is not that simple. In this chapter, we will discuss the main challenges that were experienced in a decade of netcentric crisis management in the Netherlands and formulate lessons for the future development of a netcentric information management doctrine. We base our analysis on a longitudinal research project on netcentric operations initiated in 2010 (Boersma et al., 2010, 2012; Wolbers & Boersma, 2013; Wolbers, 2016; Treurniet & Wolbers, 2021), combined with a range of studies conducted by the Netherlands Institute of Physical Safety (in Dutch: NIPV), which is responsible for supporting and developing the netcentric information management doctrine in the Netherlands (Treurniet & van Buul, 2013; van Buul et al., 2016; Treurniet et al., 2019a).

## The Concept of Netcentric Operations

The concept of netcentric information management primarily originates from developments in military command and control doctrine in both the UK and the USA (Houghton et al., 2006). In the UK, the doctrine of "Network Enabled Capabilities" was developed to improve the collaboration among military branches during expeditionary missions (Ferbrache, 2003). This new paradigm of information sharing was envisioned to improve situational awareness by developing systems to share information between the army, air force, and navy (Endsley, 1995; Houghton et al., 2006). In the USA, a similar development was undertaken, under the name of "Network Centric Warfare." Network Centric Warfare designates "*the conduct of*

**Table 1** Key tenets of netcentric operations

| | Cognitive | Information | Physical |
|---|---|---|---|
| Military domain | Self-synchronization | Superiority | Connectivity |
| Civil domain | Distributed sensemaking | Transparency | Connectivity |

*military operations using networked information systems to generate a flexible and agile military force that acts under a common commander's intent, independent of the geographic or organizational disposition of the individual elements*" (Fewell & Hazen, 2003: 2).

The idea is thus that the awareness of the military units is enhanced by sharing accurate and up-to-date information so that the units themselves are able to assess what actions to take in order to contribute to achieving the mission's objective. In that way, increased operational freedom relates netcentric warfare to the concept of "commander's intent," in which subordinates are instructed to understand the larger context of their actions, allowing them to adapt according to their own judgment in a way that is consistent with the aims of the commander (Cowper, 2000). Such local adaptations do not indicate a lack of planning (Dempsey & Chavous, 2013) but indicate that an operation should not be constrained by central command that might prevent improvisation and creativity (Mendonça et al., 2007). Over time, the doctrines of Netcentric Warfare and Netcentric Enabled Capabilities were integrated into netcentric operations, in order to encompass peacekeeping missions in addition to the focus on traditional warfare in collaboration between army, navy, and air force (Hayes, 2007).

Three central principles guide netcentric operations in military doctrine: *connectivity*, *information superiority*, and *self-synchronization* (see Table 1, the row "Military domain"). Connectivity in the network is enhanced as actors can use mobile devices to hook on to a shared information platform that allows units to get an overview of the situation and share new information with each other (Morris et al., 2007). In turn, information superiority is achieved when actors have the most actual information of the battlefield, which provides them with a decisive advantage over their opponent. Self-synchronization is achieved when the actors on the battlefield can engage in decentralized decision-making based on an up-to-date situational awareness. The netcentric platform offers units real-time information on what is happening around them, so that they can make their own informed decisions based on their commander's intent. In turn, higher echelons are able to monitor the progress and intervene whenever necessary. These three tenets thus allow for faster and more agile operations in more autonomy, because the commander is able to monitor and guide the operation on overall progress, instead of getting lost in too many operational details (van Bezooijen & Kramer, 2015). The assumption is thus that a robustly networked force increases the effectiveness of operations (Alberts & Hayes, 2003).

Despite the straightforward doctrine, the actual practice unfortunately turned out not to be that simple. The idea that there is a unified military force is misleading

(Hayes, 2007), especially in civil-military collaboration, where information needs to be shared across a wide network of disparate actors. As the concept of netcentric operations reached the field of crisis management through intensified civil-military collaboration, it turned out that networks are rarely coherent and large differences in goals, structures, and processes remained (Comfort, 2007). Crisis and disaster management in the civil domain requires acting in a network of autonomous organizations under conditions of goal consensus and, thus, is essentially a cooperative endeavor that includes processes of *distributed sensemaking*, *information transparency*, and – like in the Military domain – *connectivity* (Hayes, 2007; Moynihan, 2008) (see Table 1, the row "Civil domain").

A major challenge underlying of the tenet of self-synchronization in the military domain is that the commander's intent is often not that clear in practice, as actors sometimes have problems interpreting what the scope and translation of the intended action are (Thomas et al., 2007). This is also problematic for adopting the idea of mission command in crisis settings, as commander's intent relies on having a clear commander in chief. A key difference between a military network and public safety networks in the civil domain is that multiple organizations are interacting where stakeholders act under principles of autonomy and goal consensus (Comfort & Kapucu, 2006).

At first sight, it seems straightforward that sharing information among key actors results in better awareness during a crisis. Better awareness, in turn, results in agencies developing increasing understanding of their interdependences, thus facilitating better collaboration. However, while the adaptation of the military netcentric warfare approach to the civil domain is promising, the actual reality of netcentric information management in the civil domain turns out to be challenging. A decade of netcentric information management points to a range of key socio-technical and organizational challenges that need to be overcome.

## Development and Implementation of Netcentric Information Management

Netcentric information management was introduced in the Netherlands after the Advisory Committee ICT Coordination in Disaster Management published a critical report in March 2005. The report concluded that both the availability and the exchange of information seriously fell short in a range of response operations, such as the Enschede Fireworks Explosion in 2000, the fire in the Schiphol train tunnel in 2001, and a number of hazardous materials incidents in 2002–2004 (ACIR, 2005). A common issue in all these operations was that relevant information was not immediately recorded, not accessible to others, or quickly became distorted and incomplete through ad hoc verbal exchange. Information did not reach the people who needed it. Moreover, it turned out that strategic commanders regularly based their decision-making on outdated operational information. Strategic and tactical level commanders engaged in decision-making on issues that had already been resolved in practice. Miscommunication to the general public easily arose, and important crisis partners were often not involved in the response operation. Accordingly, in June 2005, the Dutch government used the report to initiate a renewed crisis information management system and doctrine: netcentric operations. The implementation of the system and doctrine took place in the following years across three phases. We became involved around 2009 in what would become a longitudinal study of netcentric operations that spanned across the three phases.

## *Experimental Development (2007–2009)*

In the early years, from 2007 to 2009, seven safety regions, the Ministry of Interior Affairs and the Netherlands Organization for Applied Scientific Research (TNO) engaged in the iterative development of a netcentric doctrine, supported by an information system called "Cedric" (Boersma et al., 2010). Cedric was an information system that included all the elements for building a common operational picture. It was comprised of a text and a map section, in which information about the emergency could be represented on a map by using geographical information and symbols. Subsequent versions of the doctrine and the Cedric information system were applied in exercises in which the usability and added value were assessed. This way, the netcentric doctrine and the supporting information system were iteratively developed in conjunction with the field. In various disaster simulations, it was tested what happened if the incident information was shared between response agencies. Safety regions could experiment with netcentric principles in an operational setting and experience the impact of the netcentric doctrine on their work practices.

Early results showed that netcentric operations were initially used in various ways, as several autonomous safety regions adopted their own systems and systematic. Consequently, the netcentric doctrine varied from merely focusing on information sharing, toward an enhanced decision support tool and even a shift in organization culture to a renewed concept of operations. As a response to the fragmentation across safety regions, the ministry established the "Platform Netcentric Operations" as a frontstage network for relevant actors to discuss the features of netcentric work, including its technical standards (Boersma et al., 2012).

## *Implementation (2010–2012)*

A key moment for the integration of the various concepts of netcentric operations in Dutch emergency management sector was the initiation of the Safety Regions Act in 2010. This legal framework that officially installed the safety regions also made it compulsory for each safety region to produce and share a common operational picture within a specific time frame (Safety Region Act 2010, art 2.4.1). Moreover, it legally installed the information manager as a compulsory role to the operational, tactical, and strategic command levels. Taken together, the Safety Regions Act formalized netcentric operations in the Dutch emergency management sector. The implementation of the Safety Regions Act came together in the project "netcentric work" in which the netcentric doctrine was formalized in all 25 safety regions. The project also formalized the information system itself, which to be called the "nationwide crisis management system."

The information system featured a geographical section, in which information could be represented on a map, and a text section with different pages in which all other information from different disciplines could be provided. It was configured in such a way that each emergency management discipline had the opportunity to maintain and share their own part of the common operational picture. A collective main page featured the essence of the common operational picture relevant for all emergency management agencies. New information managers were hired to operate the system during a crisis, who also embody the new information management doctrine in each safety region.

### *Netcentric Operations in Use (2013–Current)*

In 2013, the implementation project was transformed into a regular program netcentric operations, accommodated within the Netherlands Institute of Physical Safety. This program is responsible for the development of the netcentric doctrine and the information system itself. To guide this development, once every 1 or 2 years, the "state of netcentric operations" is drawn up (Treurniet & van Buul, 2013, 2014; van Buul & Treurniet, 2015; van Buul et al., 2016; de Koning et al., 2017; Treurniet et al. 2019a, b). Across these years, a number of recurring trends can be distinguished, such as the inclusion of an increasingly diverse set of crisis partners, the incorporation of preparedness and risk management in addition to the response phase, the development of information-driven command and control processes, and the generic improvement of information system capacities.

## Research Approach

This chapter is based on a longitudinal research project into netcentric operations that spans from 2009 to 2019, proving insight into key developments during a decade of netcentric operations. We first became interested in the concept of netcentric operations around 2009, when we learned about the challenges of multidisciplinary collaboration and information sharing between emergency response organizations. We conducted a range of studies into the concept of netcentric operations where we interviewed commanders and policy officers (Boersma et al., 2010, 2012). Subsequently, we were asked by the project managers of netcentric work to study the cultural and organizational characteristics required to develop netcentric operations (Wolbers et al., 2012). Through these studies, we developed our expertise on netcentric operations and followed the progression of the netcentric doctrine across the following years. We continued to develop our knowledge by developing theoretical inferences on the topics of collective sensemaking (Wolbers & Boersma, 2013), netcentric (military) doctrine (Wolbers, 2016), network configurations (Treurniet et al. 2019b), institutional design (Boersma & Wolbers, 2021), and distributed decision-making (Treurniet & Wolbers, 2021).

Parallel to this research effort, the second author was involved in as advisor in the implementation and development process of netcentric operations, resulting in (bi)annual studies into the "state of netcentric operations" (Treurniet & van Buul, 2013, 2014; van Buul & Treurniet, 2015; van Buul et al., 2016; de Koning et al., 2017; Treurniet et al. 2019a). Combined with our intimate knowledge of the netcentric development, we analyzed the recurrent challenges that were identified in these reports. We coded the themes that were mentioned in each report and used those to create categories with recurrent themes across several years. We discussed and renamed the categories together so that they reflected the major issues identified across the years as accurately as possible, which resulted in five key challenges.

## Five Key Challenges

After a decade of netcentric work in operational use (2013–2022), we observed that the doctrine of netcentric operations has been employed in a range of emergencies, crises, and disasters in the civil domain in the Netherlands. Information management turned out to be one of the core aspects of netcentric operations, adding value to collective sensemaking and situational awareness (Wolbers & Boersma, 2013), but crisis response evaluations also showed some hard-to-solve challenges. Response organizations in the civil domain (i.e., the fire service, the police, and ambulance services) are often not familiar with each other's operational procedures, routines, and ways of working and sometimes reluctant to share information with other agencies. This makes collaboration based on shared situational awareness hard to achieve. In addition, shared situational awareness in netcentric operations presupposes moving from "just" exchanging information to collaborative decision-making. A complicated factor is that in netcentric operations – depending on the kind of crisis – multiple response agencies and crisis management partners are "added" to the network, as their knowledge and expertise are needed to create an adequate crisis response organization. Finally, it is also the new type of crisis – slow burning, creeping, and protracted (Boin et al., 2020) – that puts a burden on netcentric operations. Such crises ask for a long-term commitment of agencies involved in crisis response and management. Based on our research and our engagement with the highlight, the five most pressing challenges in netcentric crisis management of the last decade have broader implications for the netcentric doctrine:

### *Maintaining an Adequate Information Position*

A recurring challenge in crisis management is how to develop and maintain an adequate information position (Boin et al., 2016). Involved agencies need to stay informed on operational progress of key actors in the response network so that they can develop and coordinate intervention strategies (Deverell et al., 2019; Treurniet et al., 2012; Pfaff et al., 2013). Yet, it turns out that in highly dynamic situations, it is challenging to codify and share relevant information in time (Schakel & Wolbers, 2021; Treurniet & Wolbers, 2021). Efforts to compile a "complete" and factual overview on a common operational picture during a crisis are destined to fail due to a crucial trade-off known as "the variable disjunction of information" (Turner, 1976). By the time information managers have succeeded in bringing together the various perspectives of different actors in a response network, the situation is likely to have changed. Indeed, as Groenendaal and Helsloot (2021) note, evaluations show that crisis managers struggle to identify outdated information or deal with multiple interpretations.

Codifying the different perspectives that emerge as a result of distributed sensemaking is difficult, as presenting information also pertains to reduction and simplification (Wolbers, 2021). Aligning different perspectives and interests under time pressure means that factual information should not only be shared on a syntactic level but also requires an interactive process to negotiate different meanings and interest on a semantic and pragmatic level, in a process that has been labeled "collective sensemaking" (Wolbers & Boersma, 2013; Treurniet & Wolbers, 2021). As time pressure builds, these more advanced levels of information exchange are likely to be sacrificed for the sake of speed. Deviating understanding and contrasting interests are likely to remain unresolved and reappear at a later stage in the operation. The key challenge is transforming information exchange among actors in a distributed network into a collaborative endeavor, in which actors engage in a continuous process of updating and questioning the significance of information to collectively tackle the crisis.

### *Reluctance to Share Information*

In each crisis, a different set of actors is brought together to collaborate in an occasional network. Each time, the composition and structure of the response network are tailored to the specific nature, progression, and scope of the crisis. The occasional nature of the collaboration implies that organizations may not be familiar with each other, or with the concept of netcentric operations (Berlin & Carlström, 2011). When organizations are not familiar with each other, this complicates their collaboration, as actors that lack trust are often reluctant to share information (Comfort & Kapucu, 2006). As such trust – the positive attitude, degree of goodwill, and reliability in the exchange of information between actors (Das

& Teng, 1998) – is a crucial aspect of netcentric collaboration (Hayes, 2007). In occasional collaborations where trust is initially lacking, it is possible to rapidly build trust together during the operation (Beck & Plowman, 2014; Meyerson et al., 1996; Quinn & Worline, 2008). Meyerson et al. (1996) adopted the term “swift trust” to denote how actors manage the vulnerability, uncertainty, and risk inherent in occasional collaborative situations. Swift trust emerges when actors develop a sense of reliability based on the visible actions or professional role execution of partners. Throughout the years of experience with netcentric operations, developing swift trust is a challenge if the netcentric platform (i.e., the technical tool) is the only means connecting the organizations, whereby there is limited room for judging a partners’ role execution, or keeping a clear view on what is done with the information that is shared with other agencies.

## *Moving from Information Exchange Toward Collaborative Decision-Making*

Information exchange between crisis response agencies is not a neutral process, as the information that is shared impacts the way crisis managers make sense of the situation and shapes how interpretations and decisions are enacted (Weick, 1988). Yet, in the early years of netcentric operations, the emphasis lied on exchange of factual information to solve the shortcomings noted in critical evaluation reports (ACIR, 2005). Crisis managers soon experienced the limits of this approach that was solely based on the exchange of factual information (Wolbers et al., 2012). The real benefits of netcentric operations emerge when the common operational picture is used to support the process of collaborative decision-making. If actors share their prognoses, intentions, and plans, other organizations and teams in the network can take these into account when making their decisions. As such, the role of a common operational picture in shaping command and control processes across the response network received more and more attention. Still, we note that the effective use of netcentric operations at the strategic level appears to be a consistent problem (Treurniet & van Buul, 2013; van Buul & Treurniet, 2015; Verheul et al., 2021). At the strategic level, the emphasis lies more on a political process of defending and negotiating policy alternatives that reflect various interests. At this administrative level, the process of information sharing is often politicized, which reflects a focus on *information superiority* instead of *transparency* (see Table 1).

### *Fostering Goal-Directed Collaboration in Larger Response Networks*

Netcentric collaboration works fairly well between a limited number of organizations that are used to the concept and are more or less familiar with each other. The initial implementation of netcentric operations in the Netherlands was focused on reaching this level of familiarity in the collaboration between the local emergency services and municipalities. Over time, more and more crisis partners in the periphery of emergency response networks encountered similar information management challenges and decided to implement the netcentric doctrine. This included waterboards, the executive agency of Infrastructure and Water Management (Rijkswaterstaat), drinking water companies, and energy supply organizations. The increase of the number of netcentric crisis partners made it necessary to improve and differentiate the access rights structure and support for dealing with large amounts of data and for linking with other information systems.

Over the past decade, the broader adoption of netcentric operations across occasional partners in the crisis management network triggered a new challenge. How to collaborate with crisis partners that are not working according to a netcentric doctrine or without netcentric information technology? Here we observe a paradox. While netcentric operations is designed to support the occasional collaboration between a diverse set of organizations, the institutionalization of the system draws a sharp line between actors using the system and actors not using the system (Treurniet et al., 2019a). It requires a big investment to adopt the netcentric doctrine, train information managers, and maintain the technology. Netcentric operations are thus less well-equipped to support information exchange and situational awareness in more spontaneous networks.

This problem intensified during the COVID-19 crisis, as collaborations between unfamiliar organizations expanded rapidly, both in number and type. First evaluations show that collaboration in a very extensive organizational network on the basis of a common operational picture is problematic (Verheul et al., 2021). This raises the question whether information exchange through a common operational picture is still feasible in such large networks. There is a risk of information overload (Bharosa et al., 2010), misinterpretation, insufficient evaluation, and validation of the information (Rake & Njå, 2009), but most importantly of an issue of reach and focus. It is challenging to interpret information properly when lacking domain-specific expertise and to reach goal consensus in the network so that information sharing facilitates network governance.

This challenge of reaching goal consensus needs some further elaboration. We argued that achieving information superiority and self-synchronization toward a commander's intent are key tenets of netcentric operations in the military domain. In contrast, the civil domain focuses on achieving a level of transparency, so that all actors are able to attain a shared level of situational awareness. The outcome of netcentric operations in the civil domain is that a collective response can be organized, based on shared awareness across organizations and command levels.

Still, a key quest in the past decade of operational use is how working on the basis of a common operational picture subsequently leads to a coherent, goal-directed collaboration. The governance of civil response networks needs to strike a balance between directive command and the facilitation of different interests across a heterogenous response network (Herranz, 2008; Boersma et al., 2021). This implies that there is no single archetypal network governance approach that matches all strategic orientations of the organizations involved (Kenis et al., 2019).

Setting up a goal-directed netcentric collaboration is thus often a challenge, as actors have different responsibilities and thus ultimately different goals that might even be in direct conflict (Boersma et al., 2021). This is visible in a range of operations across the past decade in the Netherlands, in which different agencies formulated conflicting communication messages, while communities were confronted with a serious threat (Lakerveld & Wolbers, 2020). Different actors in the Dutch response network, such as municipalities, electricity providers, or waterboards, had divergent views on the nature of the threat and required response, which were hard to solve by merely the exchange of information. Without a clear and collective overarching goal adopted across the heterogenous network, achieving goal-directed netcentric collaboration proves to be a hard-to-solve challenge.

## *Sustaining Collaboration in Protracted Crises and Risk Management*

Not only the extensiveness of the organizational network but also the *duration* of the collaboration can be problematic for effective netcentric operations. The challenge in a protracted crisis is to retain goal consensus across time when the pace and intensity of the crisis start shifting. Particularly in periods of relative calmness and stability, it can be difficult to keep each other informed without overloading each other with data and information. At this stage, setting up continuous risk assessment is warranted, as each new event does not necessarily cause an escalation of the crisis. We noted that actors struggle to assess to what extent it is necessary to keep collaborative partners informed of developments inside their own area of expertise. Moreover, longer-term collaboration opens opportunities to transform the common operational picture from a static picture into a form of structured process of data collection and analysis.

In the response to the COVID-19 crisis, we have seen many examples of this as numerous dashboards have been developed in which trends in infections, hospitalizations, deaths, vaccinations, etc., were visualized. Although such dashboards may provide valuable input, it is a pitfall that aspects that are easy to quantify are given too much weight in the decision-making process. Quantifiable input and hard data can easily outweigh qualitative information and values, while the latter may be more important in the longer term. We noted that a key challenge is to retain a balance between the type of information that feeds into prolonged collaborative decision-making cycles (Bosomworth et al., 2017; Curnin & Owen, 2013; Owen et al., 2016). As collaborations stretch over time, the inherent risk is that decision-making cycles can become isolated from outside events or partner organizations. The challenge is how to keep the long-term and short-term decision cycles integrated across time.

## Future Developments for Research and Practice

### *Increasing Connectivity of Netcentric Operations*

An important future quest is to develop a way in which new crisis partners that are not working according to netcentric principles can be incorporated into the network or find means for netcentric agencies to share information. Partly this is a problem of connectedness, as not all agencies have access to the netcentric information system, but also it is a question of opening up the practices of information sharing. The risk is that netcentric operations work only for a small set of organizations that are extensively trained, have information managers, and have adopted the netcentric systems. This stands in contrast to the unexpected and transboundary nature of crises that are likely to stretch across domains. In what ways can organizations not using netcentric operations be connected to the network and what minimal requirements are necessary for an effective information exchange that increases both situational and collaboration awareness?

As the network grows, it becomes increasingly difficult to share sensitive information as trust in the occasional network might be compromised. In essence, actors need to weigh what kind of information is shared with other organizations and civil actors in the network. This issue has already been experienced in emergency response operations with information from criminal police investigations and personalized medical information but is likely to play a larger role when response networks become more heterogenous (Schmidt et al., 2018). As such, developing formats, conditions, and strategies for information sharing in a very extensive organizational network on the basis of a common operational picture is a very relevant research area. Contemporary experiences in management of large transboundary crises such as the COVID-19 pandemic, migration, or climate change might provide valuable insights and material for renewed research in this area (Boersma et al., 2022).

### *Developing an Alternative for Self-Synchronization*

Self-synchronization is an important tenet of military netcentric warfare but has not yet found its way into the civil domain. In the military sector, self-synchronization lies at the heart of the netcentric doctrine, meaning that units use the information system to autonomously determine their own cause of action based on the commander's intent. Essentially, information management and command and control doctrine are interwoven and reinforce each other. This enables parallel processing and rapid adaptation to demands in the local context. Still, civil response networks struggle to set a clear overarching intent, due to the heterogenous nature of response networks that often struggle to achieve goal consensus (Moynihan, 2008). A robust alternative for the tenet of self-synchronization has not been found. For the future development of netcentric operations, we need to engage in a quest to determine how units can fit their own objectives into the goals set in the larger heterogenous response network. Advancement does not necessarily lie in more effective information exchange but in ways to interconnect information management and network governance so that more adaptive responses are possible. This entails using situational and collaboration awareness to develop goal consensus, but also feeding operational progress back into the decision-making cycle of crisis command teams and partner agencies.

Our own research into adaptation in emergency response has indicated that incident command should not be regarded as linear process but requires continuous switching between more centralized and decentralized modes of operation (Schakel & Wolbers, 2021). Response networks tend to transition to frontline organizing to maintain situational awareness (Endsley, 1995) and sensitivity to operations (Barton & Sutcliffe, 2009; Weick & Sutcliffe, 2011) or decouple into separate pockets of control to sustain action beyond the capabilities of the larger collective (Wolbers et al., 2018). As the command network decentralizes, its composition, connectivity, and leadership may change during the operation (Schakel & Wolbers, 2021). We thus witnessed a back-and-forth transitioning between tight coupling, loose coupling, and decoupling, which demonstrates the importance of supporting these transitions with an information sharing platform that enables organizations to retain operational functionality in demanding environments.

## *Balancing Information Transparency with Information Superiority*

A key part of military netcentric doctrine is the notion of information superiority to develop a tactical advantage against an opponent. In the civic domain, the challenge is instead to develop a level of transparency across a diverse set of actors in the response network. We noted that achieving transparency is not a goal in itself but helps to develop trust and feeds into achieving goal consensus. The challenge is that the netcentric platform may implicitly function as a means to judge a partner's role execution, feeding into the development of swift trust. Interestingly, the way, type, and amount of information are shared also tells actors belonging to other organizations much about how organizations are performing, what their focus is on, are what might be expected from the collaboration. The netcentric platform is not merely a means for information storage but also a podium to actively judge the progression of the networked collaboration itself. Achieving a level of transparency thus helps actors from different organizations to judge the quality and progression of the collaborative effort.

In contrast, at the political/administrative level, actors in the response network face a different type of interaction, where bureau-politics may feed into the existence of conflicting goals and norms in a crisis situation (Rosenthal et al., 1991). In this type of interaction, actors have benefits of achieving information superiority or framing information in a specific direction to suit their interests. Moreover, actors may decide to whether or not to share information, limit the level of detail, or whether or not to claim authority on providing valid information on a specific topic. In this respect, only having attention for achieving a sufficient level of transparency may obscure important aspects of the bureau-political nature of administrative crisis management (Kalkman & Groenewegen, 2019). For the future development of the netcentric doctrine, it offers value to see in what ways the goal of achieving optimal levels of transparency has to be weighed against the ubiquitous bureau-political dynamics in crisis response networks.

## Conclusion

In the past decade, netcentric information management has been developed into a key process for managing crises and disasters. Starting from a quest to improve information exchange among emergency response agencies, the netcentric philosophy has developed into a comprehensive information management doctrine. The core operational concept focuses on developing a common operational picture and simultaneously improving command and control processes by incorporating information managers in command teams. It is worth reflecting on how its original military tenets of self-synchronization, information superiority, and connectivity are being translated into the civil domain through distributed sensemaking and transparency. The doctrine of netcentric operations could mature toward fully fledged decision support but needs to develop ways to support interagency trust, transparency in information sharing, and a more flexible adoption among a diverse set of crisis partners.

**Acknowledgments** The third author (Kees Boersma) recognizes the support of the H2020 Research & Innovation Programme for this research under Grant Agreement "LINKS – Strengthening links between technologies and society for European disaster resilience", No. 883490

## References

ACIR. (2005). *De Vrijblijvendheid Voorbij. Op naar een effectieve multidisciplinaire informatievoorziening bij grootschalig gezamenlijk optreden in onze gedecentraliseerde eenheidsstaat*. ACIR.

Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: Command and control in the information age*. Office of the Assistant Secretary of Defense: Washington DC Command and Control Research Program (CCRP).

Barton, M. A., & Sutcliffe, K. M. (2009). Overcoming dysfunctional momentum: Organizational safety as a social achievement. *Human Relations, 62*(9), 1327–1356.

Beck, T. E., & Plowman, D. A. (2014). Temporary, emergent interorganizational collaboration in unexpected circumstances: A study of the Columbia space shuttle response effort. *Organization Science, 25*(4), 1234–1252.

Berlin, J. M., & Carlström, E. D. (2011). Why is collaboration minimized at the accident scene? A critical study of a hidden phenomenon. *Disaster Prevention and Management: An International Journal, 20*(2), 159–171.

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

Boersma, F. K., & Wolbers, J. J. (2021). Institutional design for transboundary crisis management. In *Oxford encyclopedia of crisis analysis*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1610

Boersma, K., Wolbers, J., & Wagenaar, P. (2010). Organizing emergent safety organizations: The travelling of the concept netcentric work in the Dutch safety sector. In *Proceedings of the 7th International ISCRAM Conference* – Seattle, USA, May 2010.

Boersma, K., Wagenaar, P., & Wolbers, J. (2012). Negotiating the trading zone. Creating a shared information infrastructure in the Dutch public safety sector. *Journal of Homeland Security and Emergency Management, 9*(2), article 6.

Boersma, K., Ferguson, J., Groenewegen, P., & Wolbers, J. (2021). The dynamics of power in disaster response networks. *Risk, Hazards & Crisis in Public Policy, 12*(4), 418–433.

Boersma, K., Büscher, M., & Fonio, C. (2022). Crisis management, surveillance, and digital ethics in the COVID-19 era. *Journal of Contingencies and Crisis Management, 30*(1), 2–9.

Boin, A., Stern, E., & Sundelius, B. (2016). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press.

Boin, A., Ekengren, M., & Rhinard, M. (2020). Hiding in plain sight: Conceptualizing the creeping crisis. *Risk, Hazards & Crisis in Public Policy, 11*(2), 116–138.

Bosomworth, K., Owen, C., & Curnin, S. (2017). Addressing challenges for future strategic-level emergency management: reframing, networking, and capacity-building. *Disasters, 41*(2), 306–323.

Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review, 67*(s1), 189–197.

Comfort, L. K., & Kapucu, N. (2006). Inter-organizational coordination in extreme events: The World Trade Center attacks, September 11, 2001. *National Hazards, 39*, 309–327.

Cowper, T. J. (2000). The myth of the military model of leadership in law enforcement. *Police Quarterly, 3*(3), 228–246.

Curnin, S., & Owen, C. (2013). Obtaining information in emergency management: a case study from an Australian emergency operations centre. *International Journal of Human Factors and Ergonomics, 2*(2–3), 131–158.

Das, T. K., & Teng, B. S. (1998). Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review, 23*(3), 491–512.

de Koning, L., van den Brink, P., Treurniet, W., & Suitela, V. (2017). *Staat van netcentrisch samenwerken 2017: Een eerste beeld van de netcentrische samenwerking tussen veiligheidsregio's, GHOR'en en waterschappen*. TNO.

Dempsey, R., & Chavous, J. M. (2013). Commander's intent and concept of operations. *Military Review, 93*(6), 58–66.

Deverell, E., Alvinius, A., & Hede, S. (2019). Horizontal collaboration in crisis management: An experimental study of the duty officer function in three public agencies. *Risk, Hazards & Crisis in Public Policy, 10*(4), 484–508.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32–64.

Ferbrache, D. (2003). Network enabled capability: Concepts and delivery. *Journal of Defence Science, 8*(3), 104–107.

Fewell, M. P., & Hazen, M. G. (2003). *Network-centric warfare-its nature and modelling*. Defense Science and Technology Organization: Salisbury System Sciences Lab.

Groenendaal, J., & Helsloot, I. (2021). Why technology not always adds value to crisis managers during crisis: The case of the Dutch nation-wide crisis management system LCMS. In A. Adrot, R. Grace, K. Moore & C. Zobel (Eds.), *Proceedings of the 18th ISCRAM Conference –* Blacksburg, VA, USA, May 2021.

Hayes, R. E. (2007). It's an endeavor, not a force. *The International C2 Journal, 1*(1), 145–176.

Herranz, J. (2008). The multisectoral trilemma of network management. *Journal of Public Administration Research and Theory, 18*(1), 1–31.

Houghton, R. J., Baber, C., McMaster, R., Stanton, N. A., Salmon, P., Stewart, R., & Walker, G. (2006). Command and control in emergency services operations: A social network analysis. *Ergonomics, 49*(12/13), 1204–1225.

Houghton, R. J., Baber, C., Cowton, M., Walker, G. H., & Stanton, N. A. (2008). WESTT (workload, error, situational awareness, time and teamwork): An analytical prototyping system for command and control. *Cognition, Technology & Work, 10*(3), 199–207.

Kalkman, J. P., & Groenewegen, P. (2019). On frontline workers as bureau-political actors: The case of civil–military crisis management. *Administration & Society, 51*(7), 1148–1170.

Kenis, P., Schol, L. G., Kraaij-Dirkzwager, M. M., & Timen, A. (2019). Appropriate governance responses to infectious disease threats: Developing working hypotheses. *Risk, Hazards & Crisis in Public Policy, 10*(3), 275–293.

Lakerveld, J., & Wolbers, J. (2020). *State of the art crisisbeheersing. Fase 2*. Wetenschappelijk Onderzoek- en Documentatie Centrum (WODC).

Mendonça, D., Jefferson, T., & Harrald, J. (2007). Collaborative adhocracies and mix-and-match technologies in emergency management. *Communications of the ACM, 50*(3), 44–49.

Meyerson, D., Weick, K. E., & Kramer, R. (1996). Swift trust and temporary groups. In R. Kramer & T. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 166–195). Sage.

Morris, J. C., Morris, E. D., & Jones, D. M. (2007). Reaching for the philosopher's stone: Contingent coordination and the military's response to Hurricane Katrina. *Public Administration Review, 67*(s1), 94–106.

Moynihan, D. P. (2008). Combining structural forms in the search for policy tools: Incident command systems in US crisis management. *Governance, 21*(2), 205–229.

Owen, C., Brooks, B., Bearman, C., & Curnin, S. (2016). Values and Complexities in Assessing Strategic-Level Emergency Management Effectiveness. *Journal of Contingencies and Crisis Management, 24*(3), 181–190.

Palen, L., Vieweg, S., Sutton, J., Liu, S. B., & Hughes, A. (2007). Crisis informatics: Studying crisis in a networked world. In *Proceedings of the third international conference on E-Social Science* (pp. 7–9).

Pfaff, M. S., Klein, G. L., Drury, J. L., Moon, S. P., Liu, Y., & Entezari, S. O. (2013). Supporting complex decision making through option awareness. *Journal of Cognitive Engineering and Decision Making, 7*(2), 155–178.

Quinn, R. W., & Worline, M. C. (2008). Enabling courageous collective action: Conversations from United Airlines flight 93. *Organization Science, 19*(4), 497–516.

Rake, E. L., & Njå, O. (2009). Perceptions and performances of experienced incident commanders. *Journal of Risk Research, 12*(5), 665–685.

Reuter, C., & Kaufhold, M. A. (2018). Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics. *Journal of contingencies and crisis management, 26*(1), 41–57.

Rosenthal, U., Hart, P. T., & Kouzmin, A. (1991). The bureau-politics of crisis management. *Public Administration, 69*(2), 211–233.

Schakel, J. K., & Wolbers, J. (2021). To the edge and beyond: How fast-response organizations adapt in rapidly changing crisis situations. *Human Relations, 74*(3), 405–436.

Schmidt, A., Wolbers, J., Ferguson, J., & Boersma, K. (2018). Are you Ready2Help? Conceptualizing the management of online and onsite volunteer convergence. *Journal of Contingencies and Crisis Management, 16*(3), 338–349.

Thomas, J. A., Pierce, L. G., Dixon, M. W., & Fong, G. (2007). *Interpreting commander's intent: Do we really know what we know and what we don't know*. Army Research Lab.

Treurniet, W., & van Buul, K. (2013). *De staat van de netcentrische crisisbeheersing (TNO 2013 R10515)*. TNO.

Treurniet, W., & van Buul, K. (2014). In TNO (Ed.), *De staat van netcentrische crisisbeheersing – update 2013*.

Treurniet, W., & Wolbers, J. (2021). Codifying a crisis: Progressing from information sharing to distributed decision-making. *Journal of Contingencies and Crisis Management, 29*(1), 23–35.

Treurniet, W., van Buul-Besseling, K., & Wolbers, J. (2012). Collaboration awareness–a necessity in crisis response coordination. In L. Rothkrantz, J. Ristvej & Z. Franco (Eds.), *Proceedings of the 9th International ISCRAM Conference* – Vancouver, Canada, April 2012. ISCRAM.

Treurniet, W., Suitela, V., & van Dijk, E. (2019a). *De staat van netcentrisch werken – update 2018*. IFV.

Treurniet, W., Boersma, F. K., & Groenewegen, P. (2019b). Configuring emergency response networks. *International Journal of Emergency Management, 15*(4), 316–333.

Turner, B. A. (1976). The organizational and interorganizational development of disasters. *Administrative Science Quarterly, 21*(3), 378–397.

van Bezooijen, B., & Kramer, E. H. (2015). Mission command in the information age: A normal accidents perspective on networked military operations. *Journal of Strategic Studies, 38*(4), 445–466.

van Buul, K., & Treurniet, W. (2015). *De staat van netcentrisch werken – Update 2015*. TNO.

van Buul, K., Treurniet, W., & van den Brink, P. (2016). *Eindrapportage staat van netcentrisch werken – update 2016*. TNO.

Verheul, M., van der Vlies, V., Stadhouders, L., Peeters, M., Vlagsma, J., Hylkema, D., & van Engelshoven, E. (2021). *Evaluatie van het Netcentrisch Werken tijdens de eerste maanden van de coronacrisis*. Berenschot.

Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies, 25*(4), 305–317.

Weick, K. E., & Sutcliffe, K. M. (2011). *Managing the unexpected: Resilient performance in an age of uncertainty*. John Wiley & Sons.

Wolbers, J. (2016). Enhancing network centric operations doctrine to support civil military cooperation in disaster management. In *NL ARMS Netherlands Annual Review of Military Studies 2016* (pp. 115–131). TMC Asser Press.

Wolbers, J. (2021). Understanding distributed sensemaking in crisis management: The case of the Utrecht terrorist attack. *Journal of Contingencies and Crisis Management*, early view. https://doi.org/10.1111/1468-5973.12382

Wolbers, J., & Boersma, F. K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management, 21*(4), 186–199.

Wolbers, J., Boersma, F. K., & De Heer, J. (2012). *Netcentrisch werken in ontwikkeling; een cultuuronderzoek naar multidisciplinaire samenwerking en gezamenlijke operationele beelden in de Veiligheidsregio's*. VU University Amsterdam.

Wolbers, J., Boersma, K., & Groenewegen, P. (2018). Introducing a fragmentation perspective on coordination in crisis management. *Organization Studies, 39*(11), 1521–1546.