Conference:
22nd International Command and Control Research & Technology Symposium 2017, 6-8 November, Los Angeles (USA).

Topic:
Topic 8: Methodology, Experimentation, Analysis, Assessment and Metrics

Title of Paper:
Towards the analysis, development and evaluation of NetForce Concepts, *A framework to realise NetForce concepts in tomorrow's battlespace*

Authors:
R. Benda (POC Submission Correspondence)
Research Scientist, Military Operations, TNO
Contact Information: P.O. Box 96864, 2509 JG, The Hague, The Netherlands; roy.benda@tno.n; +31 8886 64882

I.E. van Bemmel (POC Submission Correspondence)
NetForce Research Lead and Scientist, Human behavior and Organisational Innovations, TNO
Contact information: P.O. Box 23, 3769 ZG, Soesterberg, The Netherlands; Ingrid.vanbemmel@tno.nl; +31 8886 64022

N. Vink
Research Scientist, Military Operations, TNO
Contact Information: P.O. Box 96864, 2509 JG, The Hague, The Netherlands; nathalie.vink@tno.nl; +31 8886 61125

M. van Hekken
Research Scientist, Military Operations, TNO
Contact Information: P.O. Box 96864, 2509 JG, The Hague, The Netherlands; marcel.vanhekken@tno.nl; +31 8886 63928

R. Paulissen
Research Scientist, Perceptual and Cognitive Systems, TNO
Contact information: P.O. Box 23, 3769 ZG, Soesterberg, The Netherlands; rosie.paulissen@tno.nl; +31 8886 64561

J. van de Kuijt
Research Scientist, Military Operations, TNO
Contact Information: P.O. Box 96864, 2509 JG, The Hague, The Netherlands; Judith.vandekuijt@tno.nl; +31 8886 65839

J.W. Streefkerk.
Research Scientist, Perceptual and Cognitive Systems, TNO
Contact information: P.O. Box 23, 3769 ZG, Soesterberg, The Netherlands; jan-willem.streefkerk@tno.nl; +31 8886 65907

Towards the analysis, development and evaluation of NetForce Concepts

A framework to realise NetForce concepts in tomorrow's battlespace

R. Benda, I.E. van Bemmel, N. Vink, M. van Hekken, J.W. Streefkerk, J. van de Kuijt, & R. Paulissen

Abstract

Due to the increased complexity and changing character of conflicts, and various technological developments, the Netherlands defence organisation believes that a transformation of the way the military operates is imperative and that operations in networked environments, so-called NetForce operations, offer a promising new approach. During NetForce operations power and influence is achieved by connections between the different military and civilian elements in a network. Within this hybrid network, command and control as we know it will change. The commander's role shifts towards strategist, influencer and/or diplomat. Control will focus on (re-)setting the boundaries of freedom (constraints and restraints) and enabling subordinates rather than monitoring and (re-)directing subordinates 'minute-to-minute'. The idea for a NetForce concept complements and elaborates the concepts of Network-centric Warfare (NCW), Netcentric Operations (NCO) and Network Enabled Capabilities (NEC), as most research efforts within the these fields were mainly related to technological and communication challenges. NetForce research is particularly focused on challenges in the organisational and human domain with topics like command, leadership, decision-making, organisation, collaboration, manoeuvre, and information management.

In order to support a structured approach to knowledge development for (future) NetForce concepts, a NetForce Framework was developed. Within the article, the NetForce concept is described as well as three applications for the NetForce Framework: structuring knowledge gained from desk research and literature reviews; analysing real-world cases in order to identify weaknesses and threats; and supporting the development and evaluation of new NetForce sub-concepts. Conclusions are drawn about the NetForce Framework's usability for these applications.

Introduction

Today's world is a world of constant change. Megatrends like globalisation and ever-increasing digital connectivity have led to a state of global connectedness and myriad interdependencies among individuals, groups, organisations, and countries. Different geopolitical interests (e.g. power shifts), economic interests (e.g. intertwined commerce interests) and social demographic developments (e.g. rapid urbanisation) also contribute to the interdependencies that make societies vulnerable to conflict and instability. Possible sources of conflict and instability are amongst others scarcity of raw materials, poverty, illegitimate and ineffective governments, ideological conflicts, degraded humanitarian conditions, all resulting in forced displacement, migration and cultural heterogeneity.

In short, the aforementioned megatrends have led to a complex world of geopolitical, economic, and social demographic interdependencies. Complexity is visible in myriad factors and actors that

constantly interact with one another. Cause-and-effect relationships are difficult to point out and understand, debouching into unexpected shifts, changes and intentional and unintentional disruptions or so-called strategic shocks. Conflicts will be visible in the three domains: physical, information and human domain. The physical domain comprises the environment where people live, including their supporting physical objects and infrastructure, and where all physical activities take place. The information domain comprehends all elements of the information life cycle, and supporting communication and information systems and processes. The human domain is the whole of individuals and organizations with their beliefs, values, interests, purposes and the interaction between them. The significance of the information domain together with the interactions between the three domains has increased over the last years. Because developments and actions in these domains interplay, conflicts have a more hybrid character. Instability can therefore not be mitigated by military means alone. A multidisciplinary approach[1] is needed to make a difference; all possible means and combinations of actions in all three domains should be taken into account.

The changing character of conflicts and the rapid development and proliferation of new (and disruptive) technologies require new military operational concepts in order to keep operating effectively in future battlespaces. Although the basic tasks of the armed forces will continue to be part of the physical domain, the military is increasingly required to manoeuvre in all three domains: physical, human and information domain, in which collaboration with other actors is of the utmost importance. To be able to manoeuvre in all three domains, the military will need a human-centric perspective with a focus on influencing perception and on direct and indirect messaging. In order to be human centric a thorough understanding of conflict environments is important. Furthermore, adaptability and scalability become more important for accurate and timely responses to changing circumstances. In order to keep conducting successful (civil-)military operations, in a world that can be characterised as a complex and changing ecosystem, the Netherlands defence organisation believes that a transformation of the way we operate is imperative and that operations in networked environments, so-called NetForce operations, offer a promising new approach.[2]

In NetForce operations power and influence is achieved by connections between the different military and civilian elements, nodes, in a network. A NetForce concept has impact on military operations, especially the way in which the function of command and control is organised and performed. Command will be exercised within free space (provided mandate style) rather than in chains (provided order style, in a chain of command). Consequently, the commander's role makes a shift towards strategist, influencer and/or diplomat. Control will focus on (re-)setting the boundaries of freedom (constraints and restraints) and enabling subordinates rather than monitoring and (re-) directing subordinates 'minute-to-minute'. From a military perspective, a NetForce concept will therefore require new sub-concepts for the following topics: command (including 'control' aspects), leadership and decision-making, but also for organisation, intelligence, collaboration, manoeuvre, sustainment and information management and technology. A NetForce concept comprises implementation of all these sub-concepts from an organisational, human-centric and technical perspective.

[1] In a multidisciplinary approach governments, interagency partners, businesses and the public collaborate to tackle root causes of conflicts in society.

[2] This paragraph is inspired by the line of reasoning in Ascalon, the Dutch future operational concept of land operations.

The idea for a NetForce concept is not new. Research on Network Centric Warfare (NCW), Network Enabled Capabilities (NEC), and Network Centric Operations (NCO) have been performed since 1999, the year that "Network Centric Warfare, developing and leveraging information superiority", written by Alberts, Garstka and Stein was published by the CCRP. However, most research, conferences and symposia in this field were mainly focussed on technological and communication challenges such as C2 architectures, technological interoperability, and distributing situational awareness. There was less[3] attention for research from an organisational or human factor perspective. In most publications only general (often not proven) assumptions of NetForce operations have been described or presented, e.g. lack of hierarchical structure, high degree of self-synchronization, being able to disperse and aggregate rapidly, etc. To build up research on NCW and NEC , the Dutch defence organisation initiated the research program NetForce Command to develop new (sub-)concept for the aforementioned topics.

Within the NetForce Command program a **NetForce Framework** is developed that provides a structured approach to knowledge development for (future) NetForce concepts. The NetForce Framework is developed to support reasoning about potential NetForce concepts, their requirements, strengths and challenges. The NetForce framework is loosely based on existing design approaches such as situated Cognitive Engineering (sCE)[4] (Neerincx et al, 2008).

This paper describes the NetForce framework and its applications. Furthermore, we draw conclusions about its applicability for future concept development and experimentation which is necessary to support the armed forces to embrace and further develop (and eventually implement) NetForce concepts for future operations. The NetForce framework consists of seven elements that need to be considered when analysing, developing and evaluating NetForce concepts. These seven elements are: 1) trends, 2) challenges, 3) objectives, 4) concepts, 5) contexts, including boundary conditions, 6) requirements, including preconditions, and 7) effects, including (potential) strengths and weaknesses. There is not a default sequence of the framework elements that needs to be followed. The starting point and the order in which the elements are addressed depend on the application. The NetForce Framework is depicted in figure 1.

[3] Note that the human and socio-organizational dimensions of NCO are a field of scientific interest and being explored accordingly - for example, see: Pascoe & Ali (2008) - albeit to a lesser extent when compared to the technical and communications dimensions of NCO.

[4] The sCE approach involves three phases (analysis, specification and evaluation) in which requirements are specified based on an analysis of the domain, envisioned technology and human factors knowledge. Structured evaluation methods are applied to assess whether the resulting design concepts adhere to the design goals and to what extent the requirements can be supported. The NetForce framework takes a similar approach of analysing the context, defining the NetForce concepts and evaluating its effects.

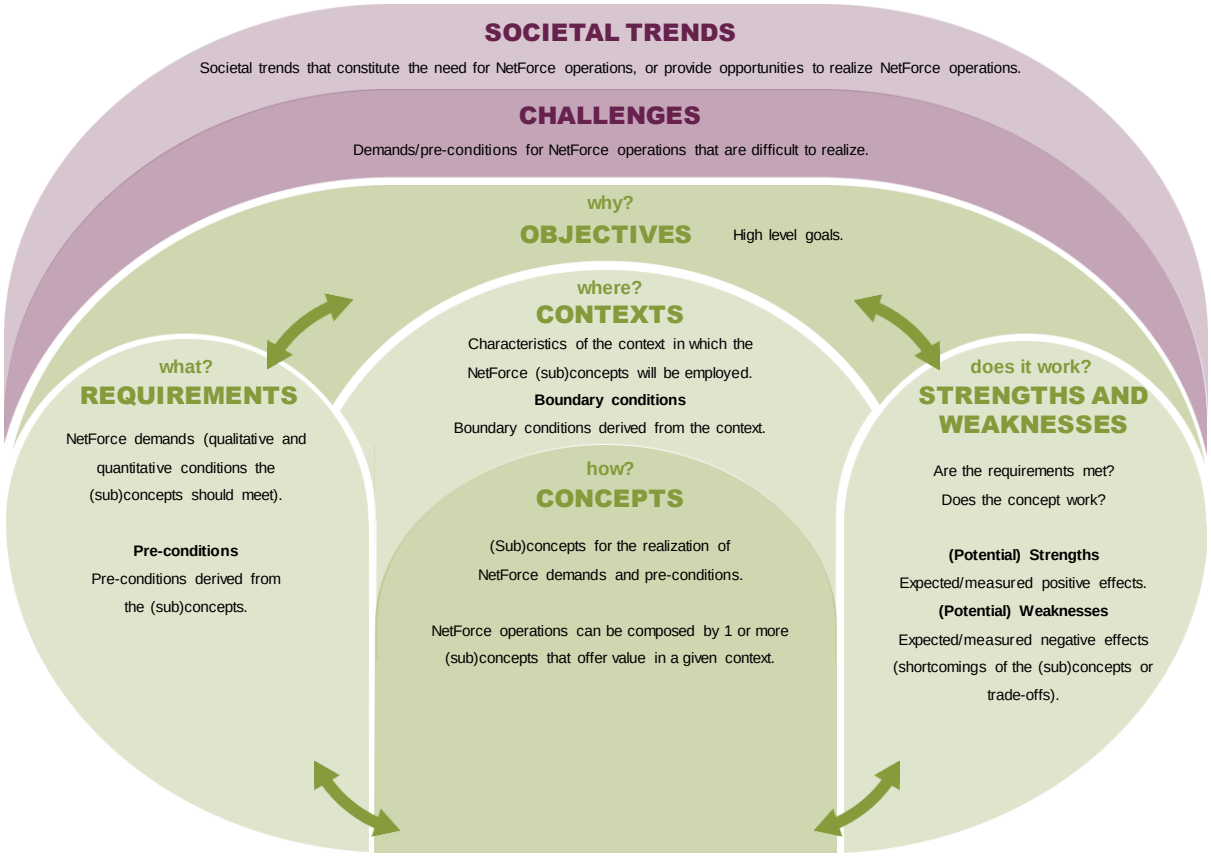

Figure 1 The NetForce framework.

The NetForce framework has three applications. Firstly, the framework can be used to analyse real-world cases in a structured way in order to draft operational scenarios and even identify weaknesses and threats. Secondly, the framework can serve as a format for structuring knowledge gained from desk research, literature reviews and case studies, and subsequently for identifying knowledge gaps. Thirdly, the framework can be used to support the development and evaluation of new NetForce sub-concepts. Further explanation of the different elements of the NetForce framework is provided in the following paragraphs which are dedicated to the three different applications of the NetForce framework.

NetForce framework for analysis of real-world occurrences

The NetForce framework can be used for analysis of real-world occurrences ('cases') in order to identify threats and opportunities for NetForce concepts. In the authors' view, these real-world cases can be either military applications of NetForce concepts or opponent applications, as long as they are adequately documented (context, objectives, effects, etc.). For illustration purposes, this section will show step-by-step how to use the NetForce framework to analyse such a case. Because of limited availability of 'success' stories from a military perspective, the terrorists perspective of the 2008 terrorist attacks on Mumbai is taken to analyse the applied concept. The perspective is based on an adequate description found in the literature, the book: Out of the Mountains by Kilcullen (2015).

Analysis of real-world occurrences with the NetForce framework starts with identifying the **societal trends** that constitute the need or provide the possibility for networked operations. An example of a

trend that makes networking a necessity is globalisation. An example of a trend that makes networking possible is the rapid development and proliferation of information and communication technology. These societal trends create all kind of **challenges**, being either opportunities or threats. The 2008 terrorist attacks were influenced by this rapid development and proliferation of information and communication technology creating a **context** with high connectivity and thus creating possibilities for a networked way of operating. The terrorist attacks took place in the densely populated area of south Mumbai, where a number of targets were selected prior to the attack. Mumbai can be characterised as a mega-city on the Indian Ocean, creating a littoral area with transnational littoral networks (shipping companies, international business networks, different ethnic groups). As Mumbai is a relatively developed area within India, global use of and access to Social Media and other digital, real-time media formats is heavily available. Using a networked way of operating the terrorists intended to disrupt public life in the city and create unrest in other major cities worldwide. This **objective** forms a starting point in using the NetForce framework. The societal trends, challenges, objective and the context related to the 2008 Mumbai terrorist attacks are depicted in figure 2.

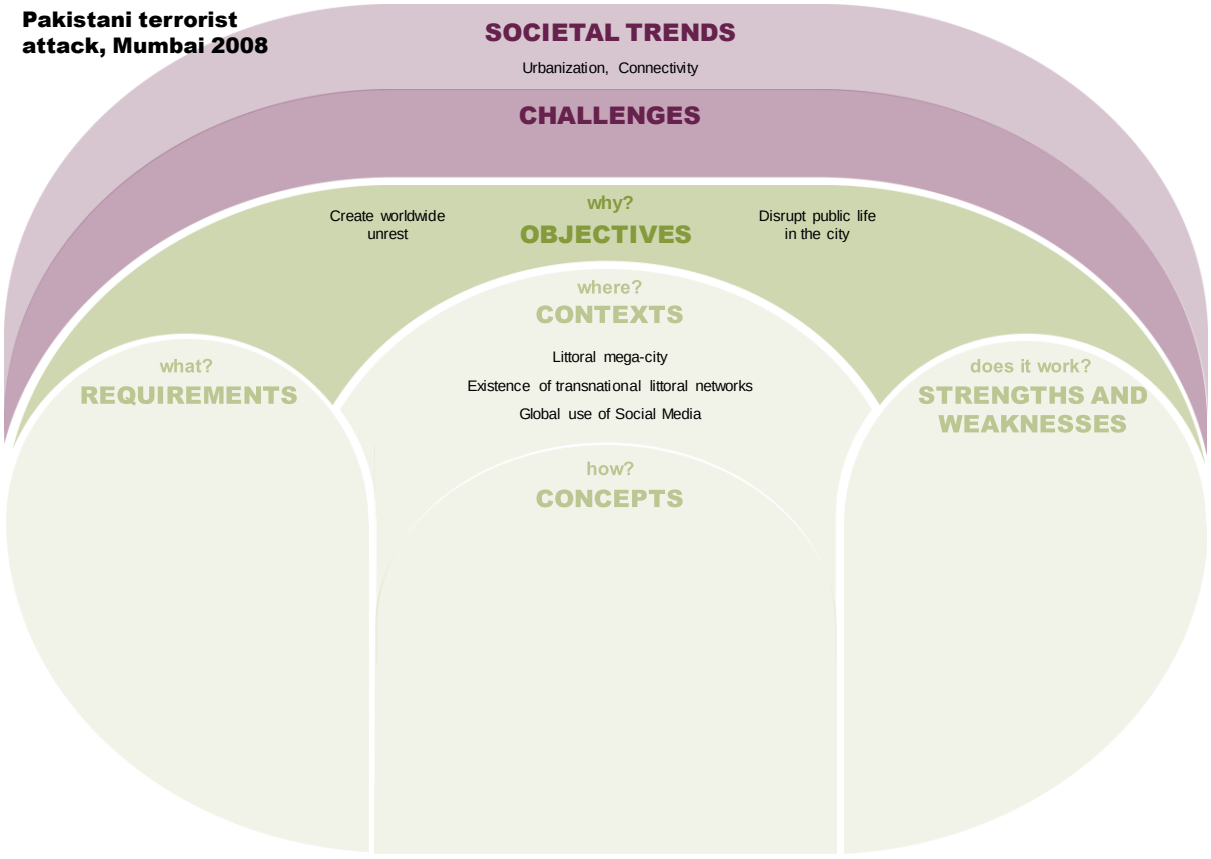

Figure 2 Framework showing the objectives, context and trends of the 2008 Mumbai terrorist attacks.

When placing these trends, objectives, and context in the framework (see Figure 2), this leads to the specification of **requirements** for how the terrorists have operated in this context. Requirements pertain to the qualitative and quantitative conditions that need to be met by the networked or NetForce concept to realise intended effects. First, in order to increase the effect of terror and urban dislocation, the response time by first responders and the crisis organisations had to be increased and preventing the authorities to respond adequately to the attack. Second, as terrorist attacks

often are propaganda-related, the attacks had to generate a lot of exposure and media coverage. Third, multiple targets had to be attacked simultaneously to prevent them warning each other and therefore maximise the effect of terror. Finally, in order for them to avoid detection prior to the attacks, they should have a low signature ('blend in') and high mobility to reach the destinations in time. See Figure 3 for the requirements of the 2008 Mumbai terrorist attack in the framework.

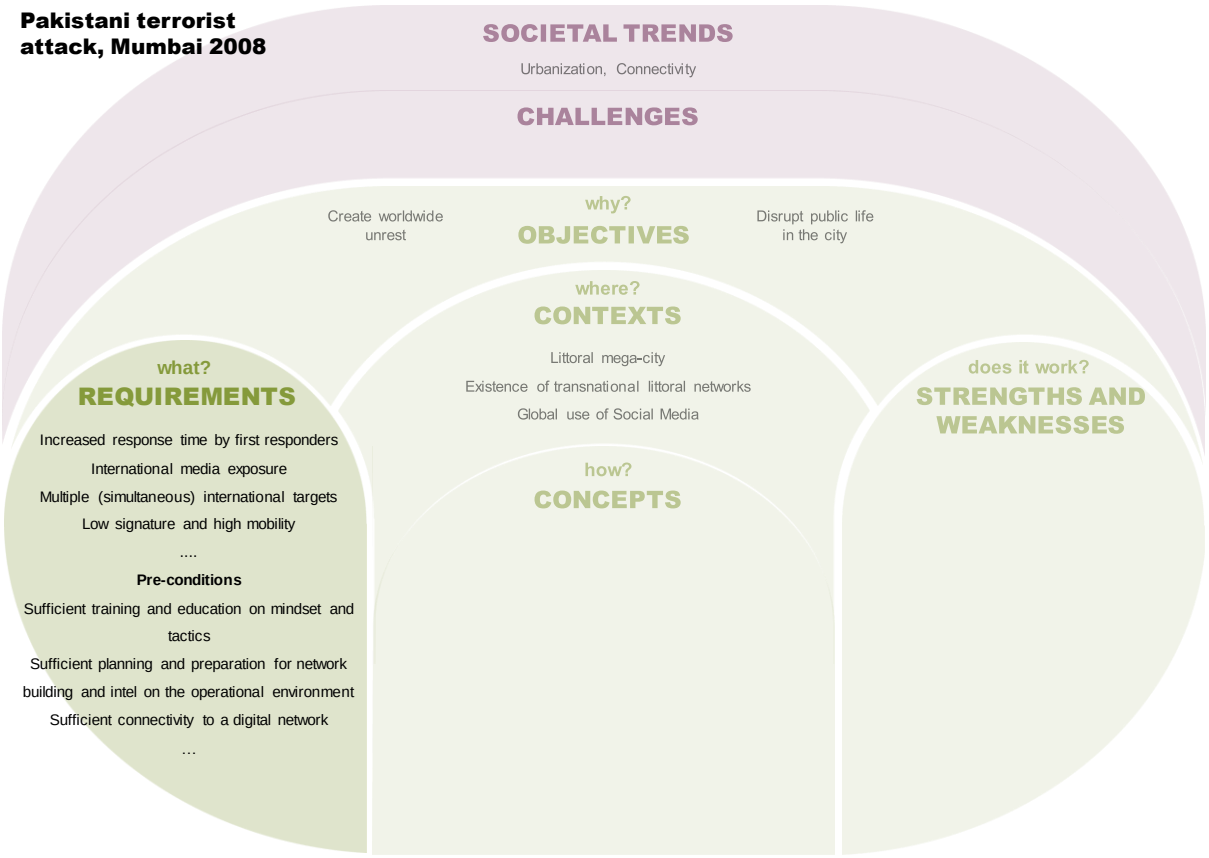

Figure 3 Framework showing the requirements and pre-conditions of the 2008 Mumbai terrorist attacks.

Central to the NetForce framework is the **concept**; the envisioned operational approach comprising of a coherent whole of smaller concepts. A concept describes (a part of) how a NetForce may operate. Note that the authors do not foresee a single overarching NetForce concept, but multiple concepts that have more or less value given the specific operational context. Concepts may relate to one or more of the following topics: command, leadership, decision-making, shared situational awareness (SA)/situational understanding (SU), information management, technology, collaboration, organisation, manoeuvre and sustainment.

The operational concept devised by the Mumbai terrorists (see Figure 4 for a short description) can be regarded in terms of some of these topics. With regard to organisation, the attackers organised themselves into a distributed swarm of small, autonomous teams. There were five teams of two attackers, without central hierarchy or hierarchy between the teams. With regard to leadership, the attackers practiced 'facilitating leadership'. Their commander was part of one of the autonomous teams and they relied on a remote command centre as a central hub to provide them with information. This command centre monitored how the situation developed to keep the dispersed teams up to date. Its role was not to issue other commands or to manage the teams' operational progress.

Transport from Pakistan to Mumbai

First the attackers hijacked one fishing trawler. Later on, when arriving Mumbai, they exchanged the fishing trawler for three military-grade inflatable boats. The assault team landed in two separate locations. The lending sites the terrorists chose were dense, complex, informal settlements. The full team of ten had landed and split into five pairs. Two of these pairs, guided by GPS, moved foot to attack their previously assigned objectives. Each of the remaining three pairs hailed one of Mumbai's taxis and blended into the traffic to move to their targets, two of these placed a IED under the seat of their taxi.

The first attacks were diversionary attacks to draw off Indian police and emergency services, forcing them to deal with multiple simultaneous incidents across the city, while the main assault force headed for its true objectives: a Jewish community centre and two luxury hotels. With chaos descending on the vast city's waterfront as the Mumbai police responded to the first attacks, the raiders were moving to their targets. During the main assault, the different assault pairs had joined to attack the hotel. The Taj Mahal staff managed to evacuate about 250 people to the hotel's chambers era. People were afraid and began sending their relatives messages on social media. The control room in Pakistan, monitoring social media, had passed this information to the attackers so that the attackers could find the hiding places. Also information on time of arrival of India's elite Marine Commando passed the attackers on the ground with the control room. When the MARCOs arrived, again the control room relayed media reports on the emergency response to the assaults teams, allowing them to stay one jump ahead of the Indian counterterrorism operators. Another hotel was being attacked synchronized with the attack on the Taj Mahal hotel. Because the police was disrupted by losses and preoccupied because of the other attack it took them four hours to arrive at the place of attack. The third target, the Jewish centre, was in one of the most densely populated parts of Mumbai. Also here, policemen lacked firepower. Again, media reported the situation (air assault) which allowed the control room in Pakistan to share this information with the terrorists. As a result it took all day to clear the house. After 60 hours of attacks, in all 172 people were killed while another 304 were injured.

Figure 4 Short description of the 2008 Mumbai attacks (Kilcullen, 2015, p.52 – p.66).

With regard to tactics, the attackers exploited transnational littoral networks as best as they could. They received support from local handlers recruited by a Pakistani terrorist group (LET) and they received training and intelligence on the operational environment by retired SOF members and Inter-Services Intelligence, the Intelligence Service from Pakistan. Their tactic was to create distraction and confusion on part of the authorities by drawing off the first response with an attack on a place without targets. For their real targets, they chose international targets to increase the media exposure of the attacks. This created the added benefit for them to be able to follow the developing situation (i.e. the impact of their raid) through digital media channels. The central command centre monitored national broadcast channels, but also social media platforms and relayed this aggregated information to the dispersed teams via text messages and voice calls. The teams themselves used Skype, cell phones and satellite phones to connect with their handlers in Pakistan. Social media allowed them to control the attacks and react as the Indian response developed. Other materials they employed were primarily small arms, IEDs, grenades and AK47 rifles.

> *"The first and clearest observation is that the raiders consciously exploited the urbanized coastal environment of Mumbai and Karachi." … "The attackers skillfully exploited the complexity of the urban environment, using slums and alleys to cover their movement between targets " (Kilcullen, p61, Out of the Mountains: the coming age of the urban guerrilla)… "The Mumbai raiders showed an extraordinary ability to exploit transnational littoral networks and*

both legitimate and illicit traffic patterns, inserting themselves into a coastal fishing fleet to cover their approach to the target. " (Kilcullen, 2015, p. 65)

These concepts led to the preconditions that should be in place before the attack could take place (see Figure 3; left hand side). **Preconditions** are a special set of requirements, which are linked to a specific concept and are mandatory to enable a successful implementation of a concept. Preconditions may relate to one or more of the DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability) factors. Preconditions of the Mumbai attacks would be that the attackers possess sufficient training and education, for example to develop the right (uniform) mindset (cf. ideological indoctrination) and to develop the required tactics (i.e. how to create proper distractions). In addition, sufficient planning and preparation must be available, with all involved actors within the network. Preparation involves having a sufficient supporting network 'on the ground' and having sufficient and reliable intelligence regarding the operational environment (e.g. location and accessibility of ports and buildings, geography, locations of first responders, and their possible routes to the locations of the planned attacks). During the raid they require sufficient and reliable information (e.g. location of first responders, location of citizens nearby the area of attack), requiring sufficient connectivity to a digital network and operators who can provide them this information. Of course, more preconditions could be stated (e.g. the operation requires a well-funded organisation to back the attackers), but the points above suffice for this illustration of the framework.

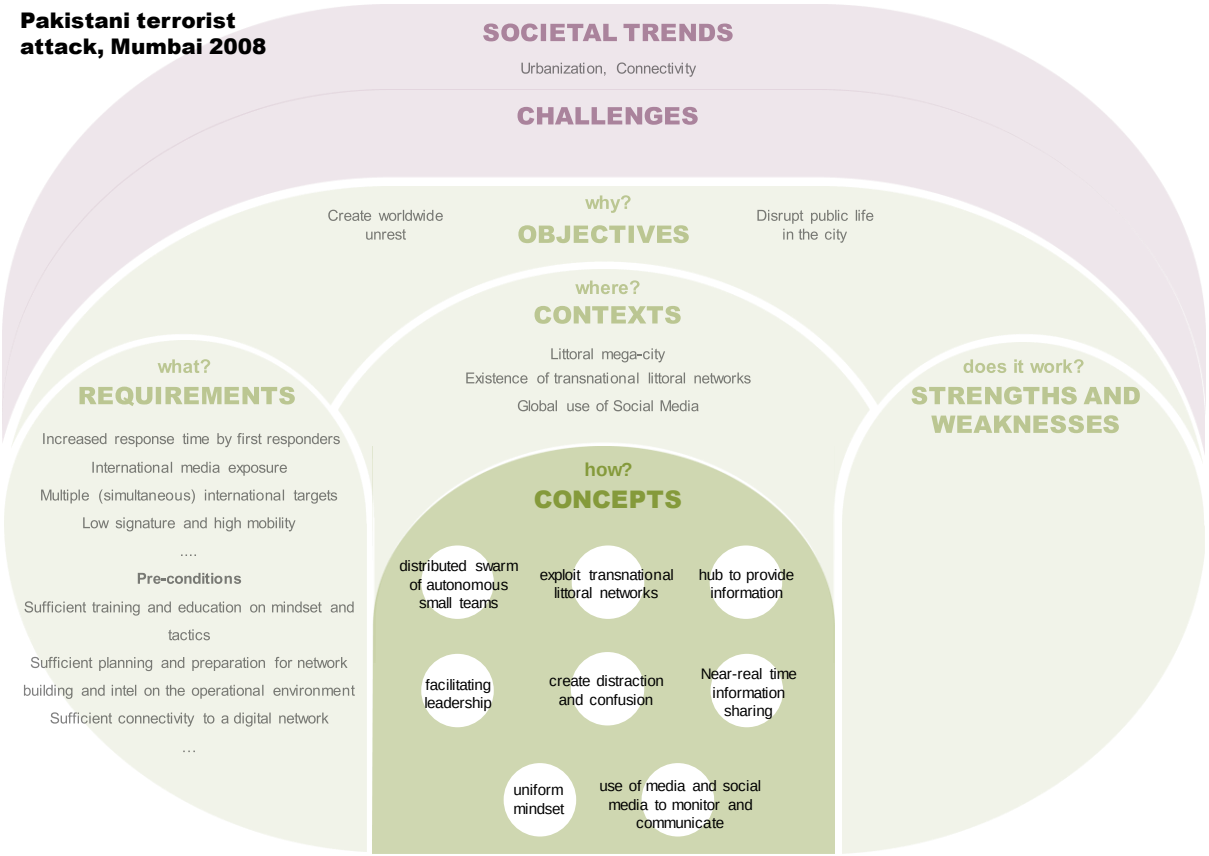

Figure 5 Framework showing the concepts of the 2008 Mumbai terrorist attacks.

Following the route through the NetForce framework (Figure 6), we can now make an assessment as to how well (in terms of **strengths and weaknesses**) the NetForce concept was capable of meeting

the objectives, requirements and preconditions**.** Strengths directly and identifiably contribute to the overall high-level goals of why the concept was employed. Weaknesses point to shortcomings of the concept or undesirable trade-offs. Identification of weaknesses can lead to a revision of the concept itself or even a revision of the requirements for the concept. In case of the Mumbai attacks, the raid attracted a lot of media coverage, owing to the fact that hotels visited by international guests were targeted. The distraction tactic and the small dispersed teams were successful in the sense that the response by first responders was delayed, fragmented and hindered by the disbanded flow of city population. As Kilcullen mentions: “The attacks on transportation and public health infrastructure also seem calculated to maximise disruption within the urban flow of Mumbai and slow the Indian response” (p.63). As can be seen from the number of injured and dead, the attacks reached their effect in number of casualties as well. In short, the direct intended effects were realised. Moreover, these effects lasted over time, as restoring order in the city took considerably longer than the attacks themselves.

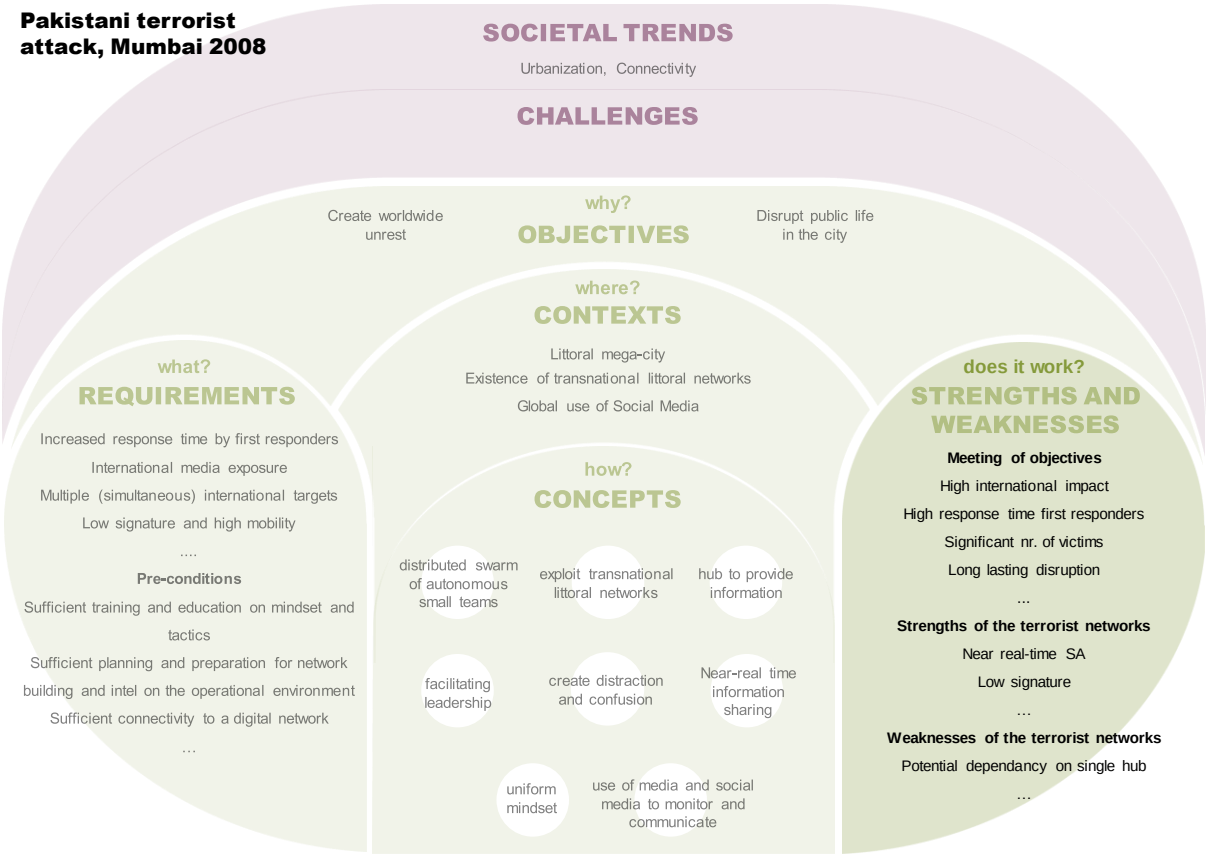

Figure 6 Framework showing the strengths and weaknesses of the concept of the 2008 Mumbai terrorist attacks.

Concerning the strengths and weaknesses of the operational concept, the attackers managed to acquire near-real-time situational awareness through readily available technology, such as simple cell phones and online platforms as well as a central hub of information. This hub did provide the potential weakness in their operational concept; a plan to fall back should have been arranged (although it is unclear what means of backup they had should their line of communication to this hub fail). Most importantly, they managed to insert themselves into the city using blending-in techniques that escaped observation until it was too late.

As illustrated by this section, the NetForce framework could be useful when conducting analyses of real-world cases in order to identify threats and opportunities for NetForce concepts. Again, these real-world cases can be either military applications of NetForce concepts or opponent applications, as long as they are adequately documented (context, objectives, effects, etc.).

NetForce framework for structuring results of a literature review

The NetForce framework can also be used for structuring the results of a literature review. The NetForce Command program reviewed military literature related to topics relevant for the development of a NetForce Concept. The review was conducted to increase insight in what NetForce comprises. The documents that were part of the military literature review differed in scope: in some documents the networked context pertains to the armed forces in a wider joint, interagency, multinational and public (JIMP) context and in other documents the networked or NetForce context comprises all the JIMP actors that operate in a certain context and contribute to a certain mission. Based on the literature review, the authors take the view that a NetForce context should comprise all the JIMP actors, meaning that the armed forces are one of the actors in a NetForce. The armed forces will need to learn how to operate effectively in a NetForce context, which is expected to differ from their own standing organisation. Note that the consequences regarding the standing organization have been placed out of scope.

The results of the review were structured with aid of the NetForce Framework. The review did not offer a complete picture of NetForce, but provided fragmented information on the different elements in the NetForce framework. Examples of the results of the literature review are depicted in Figure 7.

Many of the documents in the review offer a description of global trends and the expected context and character of future operations. Subsequently, these descriptions form the basis for reasoning about requirements and concepts for future operations. Because the descriptions contain many assumptions about the future, reasoning about the requirements and concepts for future operations is often biased in a certain direction. For example, in many papers the line of reasoning is that future conflicts require rapid deployment of small units that can operate in a dispersed manner. It is an assumption that rapid deployment, small units and dispersed operations (elements of the concept Adaptive Dispersed Operation (ADO)[5]) will be essential in all future contexts. However, in many documents, including vision documents on future forces, this assumption is interpreted as a fact and therefore not evaluated on its sensitivity before being used as a starting point for concept development. The concept of ADO may be an useful concept in some future networked contexts, but that does not mean that operations in future contexts will always comprise the ADO concept. Elaborating on this assumption, some papers also assume a close link between the ADO concept and a NetForce concept. Again this assumption may be false. The ADO concept may be part of a NetForce concept, but research needs to unravel what NetForce comprises and whether the ADO concept is always part of a NetForce concept. In short, concept development for a NetForce concept should be aware of assumptions in future context descriptions that are treated as starting points or

[5] For further elaboration, see '*Land Operations 2021 Adaptive Dispersed Operations, The Force Employment Concept for Canada's Army of Tomorrow* (Canadian Department of Defence (CAN DND), 2007).

facts. According to the authors' assessment, a NetForce concept consists of combinations of sub-concepts depending on the specific context.

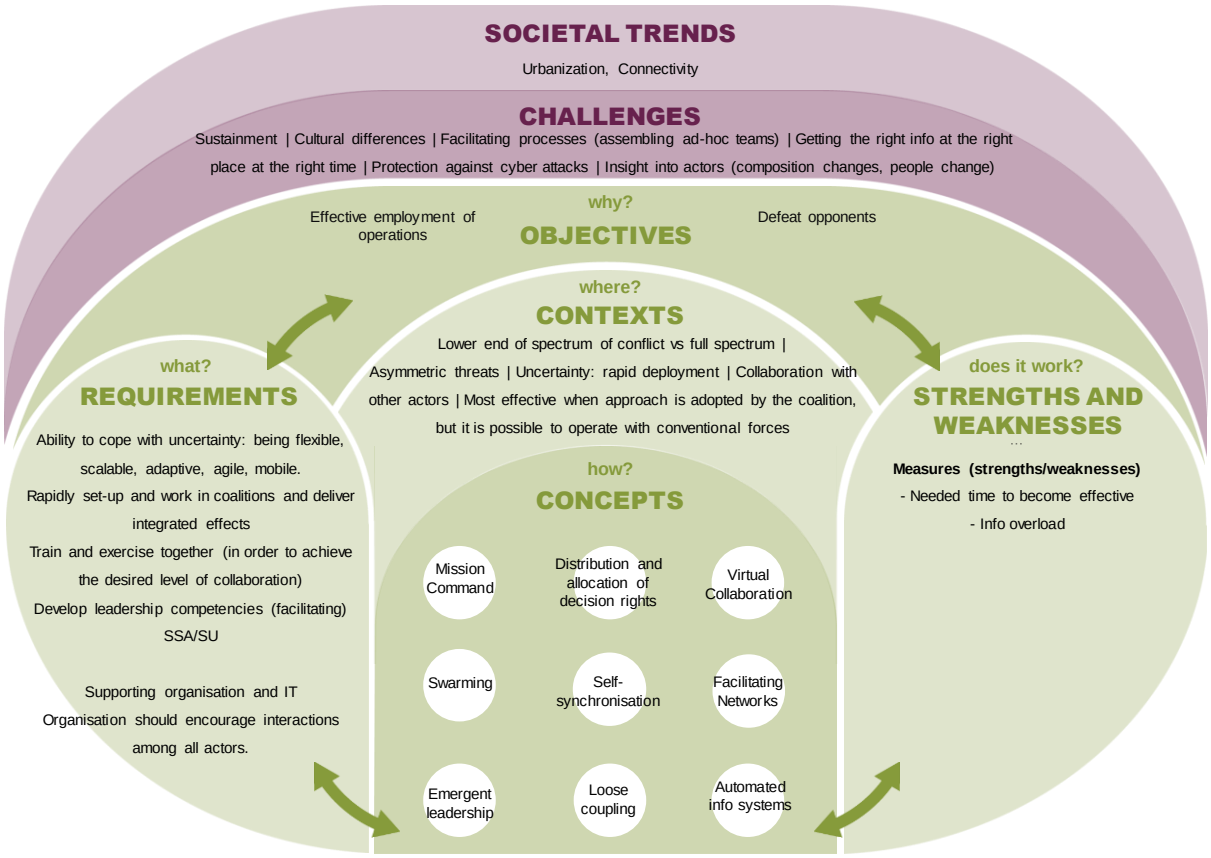

Figure 7 Examples of the results of the literature review, structured using the NetForce framework

According to the review, the future operating environment will likely be characterised by deep uncertainty, complexity, and unpredictability enabled by the global trends such as globalisation and ever-increasing digital connectivity, supported and accelerated by developments in information and communication technology. Conflicts will likely take place in complex ecosystems in which joint, interagency, multinational and public actors are involved in future operational environments. It is expected that conflicts are increasingly characterised by a hybrid blend of regular and irregular tactics intertwined in three different domains (physical, human and information). These **trends** constitute the need and provide the possibility for NetForce operations[6]

The military literature identified NetForce **challenges** which were categorized into the following topics: command, leadership, decision-making, collaboration, organisation, manoeuvre, , information management, shared situational awareness (SA)/situational understanding (SU), technology, and sustainment. The challenges related to these themes are summarized in Table 1.

[6] This paragraph is inspired by the line of thinking of Ascalon (NLD MoD, 2016) the Dutch operational concept of land operations.

Topic	Challenge
Command	Higher command levels need to facilitate lower levels, create trust and prevent micromanagement (Osinga,2007).
Leadership	Leadership needs to be redefined from traditional to virtual teams or from face-to-face expression to virtual expression, especially concerning team development and performance management (Bell & Kozlowski, 2002).
Decision-making	It must be prevented that *decision-making* takes too long, is too elaborate and time consuming. Decisions should be made best at the level where the relevant information is timely available (possibly in the field).
Organisation	It is not clear what shifting of power and liberty to lower levels will look like which complicates devising a clear vision, purposes, and division of tasks, and responsibilities (Krijgsman, 2004). It will be difficult to facilitate processes and structures in a networked environment because organisations can be assembled ad-hoc and deployed on very short notice or multiple coalitions are active at once (Beautement, 2006).
Collaboration	The ideas on what to achieve and how to achieve success are likely to differ which might prevent actors from collaborating effectively. Challenges are for example: cultural differences, differences in interests, differences in perception and rule sets, creating trust and unity of effort (Beautement, 2006).
Situational Awareness and Understanding	Insight in the behaviour of all relevant actors in an environment is never complete considering the fact that new relevant actors may appear and other actors may become less relevant, and even the behaviour, motives, reliability, interests, means etc. of actors may change in time (Taddiken, 2003). The cultural background of personnel influences how information is perceived, meaning that different commanders interpret their environment differently (Van Oort, 2015)
Manoeuvre	Note that dispersed operations could have a negative effect on both morale and unit cohesion (Edwards, 2004) and could create challenges regarding the availability of the right mix and quantities of (scarce) enablers, at the right time and place (Balasevicius, 2009) .
Information Management	The availability and usability of real-time information and – because of the increasing volume, velocity, variety and uncertainty in the veracity of data – analysing, interpreting and sharing data (Lengkeek, 2014), and preventing information overload (krijgsman, 2004).
Information Technology	Avoid implementing too specific representations of a certain 'view of the world', which may lead to (over)simplification of reality, and exclusion of other 'views of the world', other ways of working, etc. (Beautement, 2006). Protection against physical and cyber-attacks (CAN DND, 2007).
Sustainment	Sustainment in the context of logistically supporting dispersed (CAN DND, 2007) and/or high-tempo operations (TRADOC, 2014). The increased uncertainty in having (secure) access to the EM spectrum could also present significant challenges regarding the sustainment of future operations (DCDC, 2014; RAND, 2015).

Table 1 An overview of the encountered challenges

The high-level **objectives** of a network considered in the military literature review mainly concerned achieving a more effective deployment; increased combat power; higher mission effectiveness; higher operational tempo, and high-speed command. Also objectives related to force protection are addressed such as decreasing the risk of detection and decreasing the possibility of blue-on-blue. Note that these objectives are a mix of improving certain abilities and achieving goals in the operational environment.

In the literature there are different views on the **contexts** in which a networked approach seems applicable. Some state that a network is especially suited to the lower end of the spectrum of conflict and less to the higher end (Balasevicius, 2009) whereas others state a network, a netted force, is applicable to the full spectrum of violence (CAN DND, 2007; TRADOC, 2014). In general, it is acknowledged that a networked approach should be effective when dealing with asymmetric threats (e.g. COIN) (Balasevicius, 2009) and in environments where armed forces should react to uncertainty by organising themselves more loosely and by performing rapid deployment and response (Van

Bezooijen, Essens & Vogelaar, 2006; Shurkin, 2014). Furthermore, a networked approach is applicable in areas in which physically controlling an environment in itself is not sufficient or even possible; collaboration with other actors and actions in all domains are necessary to achieve success (NLD MoD, 2016). The nature of some conflicts may actually call for slow and deliberate actions, allowing other sources of national power to work as well. Letting forces self-synchronise could potentially speed the military actions ahead of the other sources of power, introducing a time gap that may hamper the other sources' ability to work (Taddiken, 2002*)*. This is an example of potential local optimization, without considering the overall objective(s), a well-known risk of self-synchronization.

In the literature review several NetForce (sub-)**concepts** were found. A NetForce concept will not be one concept ('one size fits all'). Instead it will be a handpicked combination of smaller concepts that may be combined based on the characteristics of a specific context. Examples of concepts are shown in table 2. Most of the encountered concepts are still in the early stages of concept development and not described in much detail. Often the higher objectives of the concept, the requirements (qualitative and quantitative conditions that need to be met), the intended effects, (potential) strengths and weaknesses, and the contexts in which the concept can be employed, are missing in the description of the concept. It shows that most of the concepts found in literature are still ideas that need to be developed into complete concepts and that need to be evaluated for different contexts. Table 2 shows an overview of the encountered concepts and some examples of related knowledge gaps, formulated as research questions.

Topic	**Sub-concepts**	**Examples of research questions**
Command	Mission Command (Bemmel & Essens, 2005)	How may the functions of command be implemented and organized in a NetForce without a (central) commanding agency? To what extent is control possible in a NetForce? What form may control take in a NetForce?
Leadership	Distanced and distributed leadership (Bemmel & Essens, 2005) Emergent leadership (Alberts & Hayes, 2005)	How may micromanagement be prevented in a NetForce? What are the self-managing qualities of teams or networked elements?
Decision-making	Distribution/allocation of decision rights (Alberts & Nissen, 2009) Power to the edge (Alberts & Hayes, 2005) Distributed decision-making (CAN DND, 2007)	How can local decision making be optimised without being counter-productive for the 'bigger picture'?
Organisation	Pools of capacities (Bemmel & Le Grand, 2006) Reach back (Brongers, 2008) Reverse accountability (Klinkenberg & Willigenburg, 2015)	At what organisation level should NetForce be applied (defence organisation vs whole network)? How should a NetForce organisation be organised (e.g. hierarchy levels, responsibilities)? What approach should be adopted to facilitate communication structures and processes?
Collaboration	Acting independently towards a purpose (Gouweleeuw, 2015) Virtual collaboration (Bemmel & Essens, 2005) Loose coupling (Beautement, 2006) Broad patterns of Interaction (Alberts & Nissen, 2009) Low-investment tasks (Klinkenberg & Willigenburg, 2015)	How can activities from different self-synchronized networks be aligned and to what extent do these activities need to be coordinated? How can trust be fostered among the different actors involved in order to create successful interaction?
Situational Awareness and Understanding	Knowledge workers (MacNulty, 2003) Pooling information (DSTL, 2015)	How can a large volume of real-time information about the operational environment be acquired? How can situational awareness information be shared across all involved actors at different levels

		(knowing they have different cultures and backgrounds)?
Manoeuvre	Swarming (Edwards, 2004) Self-synchronization (Bezooijen, Essen & Vogelaar, 2006) An overall concept is Adaptive Dispersed Operations (ADO) (CAN DND, 2007)	How can morale and unit cohesion be maintained when conducting dispersed operations (especially in stressful situations)? How to self-organize and self-synchronize in a NetForce? How to ensure the availability of a sufficient mix and quantities of (scarce) enablers, at the right time and place, in order to ensure the delivery of the intended (integrated) effect(s)? How to mitigate the risks associated with adopting multifunctional and modular designed units and platforms?.
Information Management	Knowledge managers (MacNulty, 2003) Broad distribution of information (Alberts & Nissen, 2009)	How may information overload be prevented in a NetForce? How may information anarchy be prevented in a NetForce?
Information Technology	Big Data Analytics	How can the vulnerability to cyber-attacks be mitigated?
Sustainment[7]	Self-reliant combat (support) units (TRADOC, 2014) A redesign of Hub-and-spoke networks (DCDC, 2012)	How may dispersed operations be sustained, reckoning with small amount of time and potential large distances between network elements and depots?

Table 2 An overview of the encountered sub-concepts and the related research questions

It needs to be determined to what extent the concepts in Table 2 are actually relevant for a NetForce context. In follow-on work all concepts must be developed and thoroughly evaluated, using the NetForce framework.

In the reviewed military literature, the ability to cope with complexity and uncertainty is addressed frequently as an important **requirement** of a NetForce concept. This includes being flexible (Beautement, 2006), adaptive (TRADOC, 2014), scalable (NLD MoD, 2016), agile[8] and mobile (CAN, 2007) in order to rapidly set-up and work in coalitions and deliver integrated effects. Therefore, networked organisations should have capabilities available to be used when required so that they can adjust to demands from the operating environment. Collaborating effectively in continuously changing networks needs an integrated approach from the start. It is important to train and exercise together in order to quickly achieve the desired level of collaboration (Keus, 2005). It also includes developing leadership competencies that will have a more facilitating character to make sure that all the actors in the network collaborate in an effective way, also when working in a distributed fashion (Bemmel & Essens, 2005). Information management plays an important role in the ability to rapidly share accurate information in order to reach shared situational awareness and understanding between actors. This calls for technical requirements focusing on realising interoperability between all actors (including their systems and procedures). A network consisting of sensors, effectors, enablers and decision-makers should be able to communicate and interact with one another, regardless of the geographical location and (type of) organisation. Therefore robust ICT-networks with sufficient bandwidth are needed as well as standardisation of procedures (DSTL, 2015; Holmes, 2009; Krijgsman, 2014). On the other hand, there are more human factor aspects that should be met, such as the willingness (mindset) to share all relevant information (Euronec Consortium, 2009).

[7] Not addressed in the previous sections.

[8] This includes C2 agility, a concept which was explored by NATO RTG SAS 85 (2014)

This willingness is essential, starting with trust among the actors. All the above requirements can only be realised when they are supported and facilitated by an effective organisation and supporting information and communication technology. The organisation should encourage interactions among all its actors, create space for individual ideas and, select and train self-directed personnel. The organisational culture should be characterised by teamwork, shared responsibilities, trust, appreciation and professionalism (Bemmel & Le Grand, 2006; Liddy, 2004). The requirements are also summarized in figure 6.

Most of the military literature that was studied emphasises the strengths of new concepts. However, now and then some possible drawbacks, i.e. potential weaknesses of the concepts were also mentioned, especially related to the concept of swarming and technology based concepts. Related to the concept of swarming several possible weaknesses are for example: the time that is needed to become effective, the high dependency on terrain and its unsuitability for the tactical defence of fixed location and borders or the attack of fixed fortifications (Edwards, 2004). Possible drawbacks of IT solutions, aimed at being able to process and distribute large amounts of data, are for example information overload (Krijgsman, 2004), insufficient bandwidth (Lengkeek, 2014) and the low usability of larger amounts of information (Alberts & Nissen, 2009). Also, the use of automated information systems is always dependent on the correct and reliable working of technology (Lengkeek, 2014). In some operational areas this might not be straightforward, e.g. within GPS denied environments. In case of technical problems, there must be a fall back / backup possibility for the most critical operational activities. Finally, a general risk of introducing IT solutions like analytics for support of human work is that humans may consider the information presented by these IT solutions as the absolute truth (Krijgsman, 2004).

As illustrated by this section, the NetForce Framework could be an useful instrument for structuring the results of a literature review and identifying knowledge gaps, especially within the context of research focused on concept development.

NetForce framework for developing and evaluating new concepts

The third and final application of the NetForce framework is to support the development of new NetForce concepts and the evaluation of new/existing concepts. This section demonstrates how the framework can be used to develop a NetForce concept by reasoning from the high-level objectives and the context. The example case of Mumbai described above shows a quite extensive description of the framework for a specific context and a specific concept. Once the framework is filled, it becomes possible to identify '**connections'** between various elements within the framework. Such a connection is shown in Figure 8, and illustrates the relations between objectives, requirements, (sub-)concepts and effects. Multiple hypotheses can be generated as to which aspects of a concept deliver the intended effects and fulfil intended objectives and which fail to do so. This will help operational concept designers to generate knowledge and creative solutions as to which concepts are potential promising approaches and how to evaluate whether they actually are.

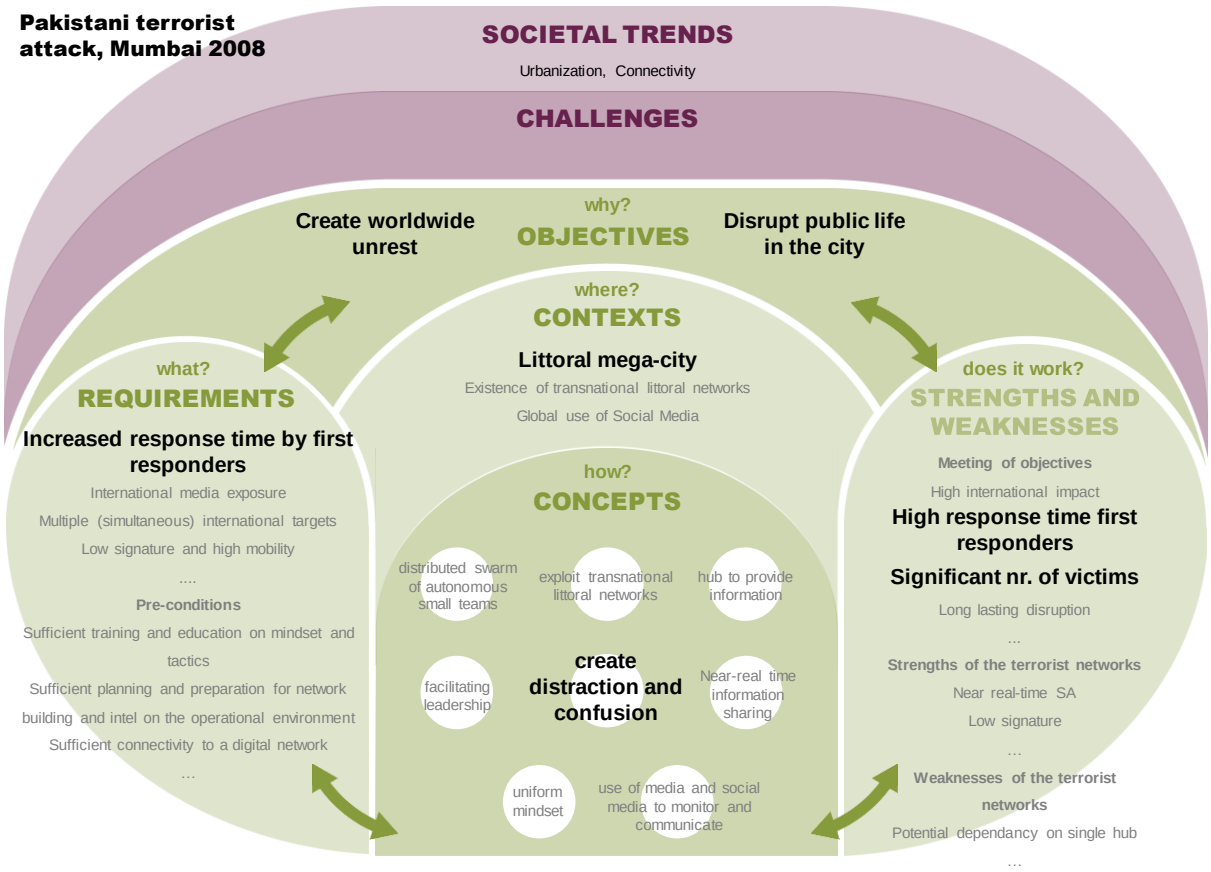

Figure 8 Visualisation of a 'connection' between various elements within the framework.

Following Figure 8, if the objective of the Mumbai raiders was to maximise the raid's disruptive impact, one of the requirements was to prevent the authorities to restore law and order quickly. Thus, the raid should increase the response time of first responders. One of the aspects of their operational concept, creating distraction and confusion, was adequately suited for this. This tactic was enhanced in the specific context of the Mumbai example: the mega-city environment with a large population. Following the connection, the tactic of creating distraction (by attacks on other than the primary targets) not only led to a long response time by first responders, but also increased the amount of victims, further increasing the disruptive effect of the attack. This is an example of a 'successful' (however tragic) connection where requirements, concept, context and strengths all enhance each other to reach the intended objective.

Identifying weaknesses or even failures in the concept applied in the example case of Mumbai were not derived from the studied literature. However, hypothetically there are so-called negative connections that do not contribute to a desired outcome. For instance, as mentioned before, a potential weakness of the concept is having a single central hub of information without a fall back plan. If for some reason sharing real-time information would have failed (e.g. the central hub of information was revealed before the attacks took place) the attackers in place had not been able to trace the hidden people, which would have supressed the disruptive impact and amount of victims.

With regard to the assessment of strengths and weaknesses, it is important to make claims on these strengths, weaknesses and trade-offs as specific as possible to be able to judge whether these effects actually occur. The rationale behind these claims needs to be verifiable. In case claims are not

met in the evaluation of a concept, requirements (e.g. conflict with the concept) or (sub-)concepts (e.g. malfunction) need to be revised. Furthermore, evaluation methods and measures need to be selected with care. The maturity of the concept determines to a large extent what methods are suitable, ranging from 'thought experiments' for very immature concepts, to evaluations in operational exercises for mature concepts. Gaming, modelling and simulation techniques could be used for the demonstration and evaluation of concepts with a mid-level of maturity. Similarly, the type of claimed strengths and weaknesses determines which measures are suitable, ranging from short-term effects to longer-term effects requiring repeated measures or complex evaluation setups. Furthermore, the necessary setting, duration, costs and personnel need to be taken into account. Where applicable, existing evaluation frameworks need to be considered for selection of appropriate methods and measures.

Conclusion

In this paper a NetForce framework is presented. The previous sections described three ways of using the NetForce framework: 1) to create insight in NetForce concepts by analysing cases 2) to structure a literature review and identifying knowledge gaps, and 3) to establish and evaluate new concepts of operation for NetForce. The authors' do not foresee a single overarching NetForce concept applicable for every context, but multiple concepts each consisting of several sub-concepts.

In applying the NetForce framework, the main challenge is to unravel the complex, intertwined relations between objectives, requirements, (sub-)concepts and (potential) strengths and weaknesses. Few of the literature we studied was able to untangle this complexity, this perhaps being the biggest knowledge gap on NetForce insights at the moment. The extent of untangling the complexity depends on the purpose and the predominant constraints (e.g. availability of capabilities and costs). This framework can provide direction in the concept development and analysis, whereas further research is needed to specify the actual implementation. On the other hand, through all kinds of methods (e.g. simulation and field exercises) a more accurate impression of NetForce can be achieved beforehand.

The NetForce framework can be applied at several levels of detail, i.e. an objective can range from a strategic focus such as 'a safer and more effective way of operating' to a more operational one as 'a higher operational tempo'. This also applies equally to the requirements, concepts and strengths / weaknesses which can be set up at different levels of detail. Note that these different levels of detail may be a consequence of the differences in orientation. Objectives, requirements and strengths / weaknesses can be oriented towards improving certain abilities or be oriented towards achieving goals in the operational environment.

Most of the encountered promising concepts as described in this paper are just briefly described in literature. Future work needs to develop and thoroughly evaluate concepts applicable in a NetForce. The introduced NetForce framework can support the analysis on potential concepts to give direction to the (DOTMLPFI) consequences (in terms of preconditions) of a NetForce concept. In order to make the NetForce framework more applicable and widespread available, future work should focus on further method development of the implementation of the elements. The examples provided in this paper to categorise the elements of the framework - i.e. PMESII-PT for specifying the context - can serve as a starting point in future work.

References

- Alberts, D.S., Garstka, J.J. & Stein, F.P. (1999). *Network Centric Warfare, developing and leveraging information superiority.* Washington D.C.: CCRP
- Alberts, D.S. & Hayes, R.E. (2003). *Power to the Edge, Command & Control in the Information Age.* Washington: CCRP
- Alberts, D.S. & Nissen, M.E. (2009). Toward Harmonizing Command and Control with Organization and Management Theory. *The International C2 Journal,* Vol 3, Nr. 2.
- Balasevicius, T. (2009). Unconvential Warfare: The missing Link in the future of Land Operations. *Canadian Military Journal*, Vol 9 (4), p. 30-40.
- Beautement, P. (2006). *Agile and Adaptive Coalition Operations - Leveraging the Power of Complex Environments.* Paper presented at 11th ICCRTS: Coalition Command and Control in the Networked Era.
- Bell, B.S. & Kozlowski, S.W.J. (2002). *A Typology of Virtual Teams: Implications for Effective Leadership.* Paper submitted to Cornell University IRL School.
- Bemmel, I.E. & Essens, P.J.M.D. (2005). *Competencies of Future Commanders in Network Centric Operations.* Paper presented at 10th ICCRTS: The Future of C2.
- Bemmel, I.E. & Grand, N.P. le. (2006). *Competenties van commandanten in een NEC omgeving (TNO-DV3 2006 A051.* Den Haag: TNO
- Bezooijen, B.J.A. van, Essens, P.J.M.D. & Vogelaar, A.L.W. (2005). *Military Self-Synchronisation, an Explanation of the Concept.* Paper presented at 11th ICCRTS: Coalition Command and Control in the Networked Era.
- Brongers, D.M. (2008). Network Enabled Capabilities bij het grondoptreden. *Militaire Spectator, Jaargang 177, Nr. 11.*
- Canadian Department of National Defence. (CAN DND) (2007). *Land Operations 2021 Adaptive Dispersed Operations The Force Employment Concept for Canada's Army of Tomorrow*. Kingston, Ontario: Directorate of Land Concepts and Design.
- DCDC. (2012). *Joint Concept Note 2/12 Future Land Operations Concept.* Shrivenham: DCDC.
- DCDC. (2014). *Global Strategic Trends – Out to 2045*. Shrivenham: DCDC.
- DSTL. (2015). *LEFC Conceptual Force Wargame – Flash Report.* Fareham: DSTL.
- Edwards, S.J.A. (2004). *Swarming and the Future of Warfare*. Santa Monica: RAND Corporation.
- Euronec Consortium. (2009). *Extract from the NEC Vision, EU NEC Vision Report.*
- Gouweleeuw, R. (2015). *150925 Netforce wargame - verslag RG.* The Hague: TNO.
- Holmes, M. (2009). NATO Chief Discusses Bandwidth Management, Shift to IP Technology. *Via Satellite.* Available: http://www.satellitetoday.com/telecom/2009/01/09/nato-chief-discusses-bandwidth-management-shift-to-ip-technology/
- Keus, H.E. (2005). *Netforce Principles: An Elementary Foundation of NEC for Creating Joint Netcentric Environments.* Paper presented at 10th ICCRTS: The Future of C2.
- Kilcullen, D. (2015). *Out of the Mountains, the coming of age of the urban guerilla.* New York: Oxford University Press.
- Klinkenberg, J.C. & Willigenburg, M.B. (2015). De toekomst van de luchtmacht: een hoofdrol voor sociale innovatie. *Militaire Spectator (jaargang 184, nr. 6).*

- Krijgsman, P.J. (2004). *Studie 'Network Enabled Capabilities (NEC)', Netwerkend Optreden - Eerste stap van conceptuele visie naar praktijk.* Den Haag: Ministerie van Defensie (NLD MoD).
- Lengkeek, V. (2014). *CLSK C4ISR-visie.* Breda: Royal Netherlands Airforce.
- Liddy, L. (2004). The Strategic Corporal; some requirements in training and education. *Australian Army Journal,* Vol 2, nr. 2.
- MacNulty, C.A.R. (2003). *Critical Human Elements of Future Warfare.* Paper contributing to RAP Report # 04-01, JFCOM J9 Project Alpha.
- NATO (2014). *C2 Agility, Task Group SAS-85 Final Report.* Brussels: NATO
- Neerincx, MA & Lindenberg, J (2008). Situated cognitive engineering for complex task environments. In *Naturalistic decision-making and macrocognition* (pp. 373-390).
- NLD MoD. (2016). *Ascalon, Operationeel Concept voor het Landoptreden*. Amersfoort: Land Warfare Centre.
- Oort, K. van, (2015). *An Analysis of the Implication of the NetForce Concept on the NLD tactical-level intelligence organization.* A Master thesis submitted to the faculty of American Public University System.
- Osinga, F. (2007). *John Boyd and Strategic Theory in the Postmodern Era.*
- Pascoe, C. & Ali, I. (2008). Taking power to the edge with Network Centric Warfare and the new Command and Control: an Australian Perspective. *Australian Defence Force Journal, Issue 176, 34-46.*
- Shurkin, M. (2014). *France's War in Mali, Lessons for an Expeditionary Army.* Santa Monica: RAND Corporation.
- Taddiken, B.C. (2003). *The Cultural Challenges of Joint Self-Synchronisation.* A paper submitted to the Naval War College. Newport: Naval War College.
- TRADOC (2014). *Win in a complex world (2020-2040).* US Army: TRADOC.