NETFORCE COMMAND

AN ALTERNATIVE FOR HIERARCHICAL COMMAND AND CONTROL IN COMPLEX, DYNAMIC AND NETWORKED MISSION ENVIRONMENTS

Authors
Ingrid van Bemmel
Marcel van Hekken
Rosie Paulissen
Aletta Eikelboom
Judith van de Kuijt
Roy Benda
Lisa Ziekenoppasser

TNO innovation for life

NETFORCE COMMAND

AN ALTERNATIVE FOR HIERARCHICAL COMMAND AND CONTROL IN COMPLEX, DYNAMIC AND NETWORKED MISSION ENVIRONMENTS

TABLE OF CONTENTS

NOTE FROM THE AUTHORS

NetForce Command – An alternative for hierarchical command and control in complex, dynamic and networked mission environments describes the results of a four year TNO research programme, V1604 NetForce Command, that was carried out by TNO in collaboration with the Land Warfare Centre of the Royal Netherlands Army. The objective of the research programme was to develop a NetForce Command concept that provides the armed forces of the Netherlands with the opportunity to contribute and operate effectively in the complex, dynamic and networked environments in which their missions will take place in the future.

The NetForce Command concept is the outcome of a thought experiment from different angles. When developing the NetForce Command concept, we realised that it is a concept for a future that we could not really know or predict. We could only use current trends and analyses of foreseen mission environments as inspiration. We also knew that we could not reach a final conclusion during the course of the research programme. Therefore, in this book, we describe and consolidate our findings of four years of thinking about NetForce Command.

This book provides the building blocks for the expansion of current command and control doctrine and the implementation of NetForce Command. The book is meant to inspire, to stimulate further conceptual thinking about NetForce Command and to encourage experimentation with different aspects of NetForce Command. We intend to make you wonder, to stimulate debates, to raise questions, to give you feelings of uneasiness, astonishment or even anger, because that can eventually lead to the implementation of NetForce Command.

Instead of reading the book in a linear fashion, you can read the book as a NetForce. We recommend to start with chapter 1 and 2, but thereafter you can chose any chapter you like. In a way, you can swarm through the book and begin your own NetForce Command thought experiment.

We wish you a pleasant journey, reading this book!

The authors

SECURITY THROUGH FORESIGHT

The world around us is changing at a rapid pace. Technological and economic developments are creating increased interconnectivity. Meanwhile, not only new threats are continuously emerging but also old threats are manifesting themselves in new and deceptive ways. Armed Land forces have already played an important role as a national instrument of politics for ages. But they need to keep up with the pace of ongoing change, if they are to continue their relevant role, let alone to be of decisive importance in the future. Even more it is absolute essential that they are able to predict what is expected, to analyze what could happen and then deduct what is required, in order to deal with any situation at hand.

The Land Warfare Centre of the Royal Netherlands Army is continuously working on conceptual innovation and development. Derived from the changes in the mission environment, we must seek out our assigned and desired role, adjusted and adapted to the expectations of others. This will direct our capability development and guidance for the way we will be required to operate in the future. Seeing ourselves as part of a NetForce, we cannot make a decision about this on our own. Whether it is about our national whole of government approach, the international security organizations to which we contribute, or any other form with new actors which we cannot even comprehend right now.

We are therefore very proud that the results of a four year integrated study has led to new and alternative models and forms of command and control in missions in order to bring and restore security and stability. The theory and new insights which we gained, can be used and implemented when organizing command and control in the challenging future combat environment. People, processes and means need to be prepared and adjusted in order to stay relevant.

Since you have a copy of this book and have started to read it, it is clear that you possess the open-minded attitude which is fundamental to counter the natural reluctance of humans to change. Enjoy the read and I encourage you to discuss the questions which remain, for it will help us to improve.

Commander Land Warfare Centre,

Henk de Boer
Colonel of the Fusiliers

INTRODUCTION TO NETFORCE COMMAND

1

1 INTRODUCTION

All military officers are educated and trained in command and control. Right from the start of their education and training at defence academies, military officers are taught and skilled to become commanders. Directly after their education they start as commander of a small unit, followed by several other command functions during their career. Consequently, each military officer is trained in command and control, often with hands-on experience in the field, and will have examples, ideas, and opinions about what will make a good commander.

A book on command and control in future mission environments is therefore a hazardous challenge that can only be done when applied scientists work in close collaboration with military officers. And that is exactly what TNO did in collaboration with the Land Warfare Centre of the Royal Netherlands Army. The past four years we collaborated and developed an alternative for a hierarchical approach of command and control: NetForce Command. This networked alternative is not to replace, but to complement the hierarchical approach of command and control, specifically for complex, dynamic and networked mission environments in which a high operational tempo, agility and harmonisation of effort are essential.

The NetForce Command concept that we describe in this book is based on a four year research programme, V1604 NetForce Command, that TNO carried out in collaboration with the Land Warfare Centre and many other military officers in the NetForce community who thought-along during the course of the research programme. The objective of the research programme is to develop a NetForce Command concept that provides the armed forces of the Netherlands with the opportunity to operate effectively in complex, dynamic and networked mission environments. More information on the NetForce Command research programme is included in annex A. The development of the NetForce Command concept has been an extensive thought experiment. This book presents the results of that thought experiment, provides the building blocks for the expansion of current command and control doctrine and the implementation of NetForce Command. The book is meant to inspire, to stimulate further conceptual thinking about NetForce Command and to encourage experimentation with different aspects of NetForce Command.

> **"The objective of the research programme is to develop a NetForce Command concept that provides the armed forces of the Netherlands with the opportunity to operate effectively in complex, dynamic and networked mission environments."**

Instead of reading the book in a linear fashion, the book can be read as a NetForce. However, we recommend to start with chapter 1 and 2. In this chapter 1 we provide a short introduction to NetForce Command, including a description of future mission environments, their challenges for the armed forces, the potential shortcomings of a hierarchical approach of command and control and a description of NetForce and

NetForce Command. In chapter 2 we dive deeper into NetForce Command and describe how different implementations of NetForce Command, varying from maximum self-synchronisation to maximum orchestration, depend on the composition, organisation and structure, and interaction in NetForce. After reading chapter 1 and 2 you can chose any chapter you find interesting. If you want to have an impression of future NetForce Operations, we recommend to continue with chapter 5, which introduces a potential form of NetForce operations, hybrid swarming. If you want to get a grasp of what NetForce Command may look like, we recommend to read chapter 4, in which interviews with future actors take you on a tour of NetForce Command. If you want to gain more in depth knowledge of NetForce Command, we refer to chapter 3 in which we describe different aspects of a networked approach to command and control: self-synchronisation, orchestration, leadership, decision-making and information-management. If you want to get an idea of what a potential implementation of NetForce Command means for the armed forces, you can read about the implications in chapter 6. In a way, you can swarm through the book and begin your own NetForce Command thought experiment.

1.1 The complexity, dynamics and networked character of future mission environments

The foreseen future mission environment can be described as complex and dynamic. In this environment developments, threats and opportunities are unpredictable. Globalisation and advances in information and communication technology have led to a complex society with global connections and interdependencies. There is an ongoing stream of new forms of digitalisation that, amongst other things, enables individuals to be connected and socially networked, to have unlimited access to information and to transfer information freely. Furthermore, increased urbanisation, large differences in social-economic perspectives, the effects of aging populations and increasing regional birth rates have effects on worldwide migration and further increase the interconnectedness. Faster than we might have thought, our society has become a complex network of individuals, groups, organisations and communities in which events, actions and activities are intertwined and globally connected.[1]
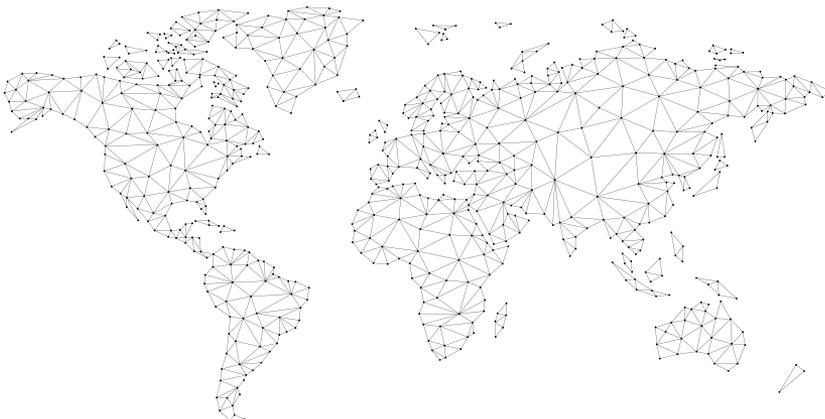
Figure 1 Globally connected world

---

1. For the development of a NetForce Command concept and the description of the foreseen future mission environment we mainly used Deducties voor het landoptreden: *editie Silene* (2015) of the Land Warfare Centre of the Royal Netherlands Army. Undoubtedly, other countries have similar documents describing future mission environments.

The emergence of new technologies and social software seems both promising and frightening at the same time (De Spiegeleire et al., 2017). It allows us to have widespread communication and easy access to information, but opponents or malicious actors have become extremely good in using the possibilities of the hyperconnected and socially connected world as well. The increased interconnectedness leads to more obscure and complex mission environments and therefore an increased level of uncertainty with regard to opponents and other actors, types of missions, operations, coalitions and the mission environment.

The increased rate of development and proliferation of both knowledge and technology (for example automation, unmanned systems, quantum computing, etc) in combination with the increased rate of interconnectedness could lead to fast and effective adoption of new modus operandi or technologies by opponents and thereby adds to the unpredictability of their behaviour. This fast adoption can for example be seen in the increased number of proxy-wars where powerful (near-)peer opponents support local actors (as is the case in Syria). Furthermore, the increased amount of conflicts involving non-state actors contributes to an uncertain mission environment. This means that conventional methods of warfare might not always be suitable when engaging non-state actors, as can be seen during recent Counter Insurgency (COIN) operations in Iraq and Afghanistan. The strategy and corresponding set of activities that is required to effectively engage these actors can be obscured for extended periods of time and may change quickly during engagement. The same holds for countering hybrid threats, such as the annexation of Crimea or the rise of ISIS. Hybrid activities are a combination of activities in the physical, human and information environment.[2] The links between different activities are often unclear and therefore hard to detect. In such contexts, conventional as well as non-conventional means and activities, and ethical values and standards, are employed.
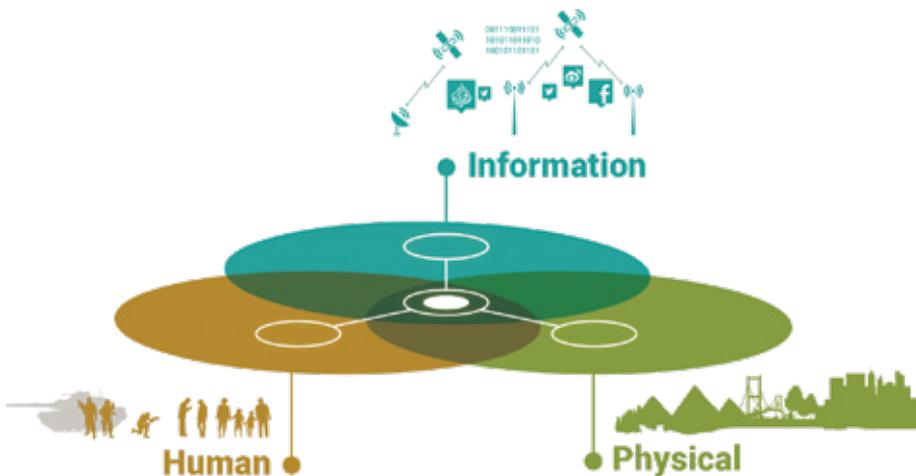
Figure 2 Three environments model (Land Warfare Centre, 2017)

---

2. The physical environment comprises the environment where people live, including their supporting physical objects and infrastructure and where all physical activities take place. The information environment comprehends all elements of the information life cycle and supporting communication and information systems and processes including data (-manipulation) and cyber. The human environment is the whole of individuals and organisations with their beliefs, values, interests, purposes and the interaction between them (Land Warfare Centre, 2017).

The increased rate of interconnectedness also leads to expansion of the battlespace. Conflicts no longer pertain to a limited physical area, but to a global battlespace where information, knowledge, perceptions and ideas can spread rapidly. Consequently, homeland safety and security have become intertwined with safety and security in other parts of the world. Instability cannot be mitigated by military means alone; it requires involvement of different actors across different areas (e.g. political, military, economic, social, infrastructure, information). All instruments of power and possible combinations of actions in all three environments need to be considered.

These foreseen future mission environments require a higher operational tempo, agility and harmonisation of efforts of different actors in the three environments in order to achieve desired effects and outcomes. These requirements pose several challenges and demands to the armed forces. In the next section these challenges and demands are discussed.

1.2   Armed forces are challenged

The armed forces and international organisations like NATO and EU are extremely well designed for state-to-state conflicts in the physical environment. However, they will increasingly lag behind what is required in the foreseen future mission environments. The armed forces need to adapt in order to be able to successfully tackle their challenges. To be more specific, the conduct of operations increasingly demands for more internal as well as external Situational Awareness (SA) and Understanding (SU), a high(er) level of flexibility and adaptability from the armed forces, and increased collaboration and interoperability with a wide variety and large amount of actors. Moreover, the assumption is that future mission environments also demand an integration of different instruments of power[3] and a higher operational tempo. In the remainder of this section we describe these four demands in more detail.

The foreseen mission environment as described in the previous section demands the availability of a superior information position. Armed forces are required to have a thorough understanding of different actors' goals, interests, relationships with other actors in order to effectively lead, make decisions and direct, organise and coordinate their efforts. Situational Understanding is the condition in which there is an understanding of what needs to be done to accomplish the mission. But even more so, Situational Understanding facilitates the interaction process between capabilities to find each other, to link up and harmonise for a specific activity.

Adaptiveness is a fundamental characteristic in a dynamic and uncertain security environment (Sweijs et al., 2018). To adapt is defined as 'being able to change or be changed in order to fit or work better in some situation or for some purpose' (Merriam-Webster's Learner's Dictionary, n.d.). Consequently, in the face of complex and highly dynamic threats and challenges, being flexible and adaptive is arguably one of the defining demands of an effective military contribution. Armed forces need to be able to operate in a wide range of mission types (be flexible) and be able to adapt to changing operational circumstances or changing operational and functional requirements (be adaptive).

---

3.   For example, military, social, economic and diplomatic instruments

In the foreseen future mission environment, collaboration and interoperability with a wide variety and large amount of actors will be significant. Firstly, the various nation's branches of the armed forces (Army, Navy and Air Force) are increasingly required to work together in order to operate effectively, i.e. conduct multidomain operations. Secondly, international military collaborations become a necessity, especially for smaller nations. Smaller nations have to ensure national security, which is increasingly challenging because of the relatively small size of their armed forces and budgets in the past years. Furthermore, expeditionary armed forces are increasingly cooperating with local armed forces during operations, e.g. when delivering military assistance in support of local ground forces as can be observed in the current conflict in Syria. Combined operations are increasingly important. Lastly, since the complexity of conflicts and missions increases, interaction and collaboration with other departments and agencies, non-governmental organisations, local population and local (political) leaders will become more important in order to deliver an effective and sustainable resolution. This potentially varied and large civil-military coalition of Joint, Interagency, Multinational and Public (JIMP) actors is likely to be characterised by the presence of partially overlapping and sometimes contradicting interests and goals; the use of a wide variety of systems, processes and procedures; and the conduct of a wide variety and amount of individual activities. Nevertheless, in order to deliver effective and sustainable changes in the foreseen mission environment, this coalition of JIMP actors is required to harmonise their activities and to create unity of effort.

It is expected that actors in armed conflict will be competing more explicitly across the physical, human and information environment. Armed forces are faced with the challenge of opponents that employ a mixture of conventional and unconventional means. Actors are rebuilding and modernising their different instruments of power, including non-kinetic instruments, to gain advantage of competitors (Sweijs et al., 2018). Alternative and hybrid strategies without direct military confrontation are increasingly being used to expand one's own power or hinder the power of others, or to paralyse military deployment (Land Warfare Centre, 2015). Armed forces will become increasingly pressured to find their role in an effective response to these threats. Therefore, armed forces must interact and collaborate with different instruments of power, both military and non-military, to reach an optimal result.

During the exercise Deep Strike 2018 it became apparent that future opponents will often have a higher tactical pace compared to current western armed forces. Most western armed forces are traditionally more static/linear oriented and therefore relatively slow in creating effects. Armed forces, therefore, must be quickly deployable to be able to successfully tackle this challenge. Quickly deployable assets would not only allow to support fast strategic mobility and a flexible battle, but also enable armed forces to achieve tactical surprise (Royal Netherlands Army, 2018). (Forward) Command Posts also need to be able to quickly move from one location to the other to become more mobile, speed up the OODA-loop, and to keep up with the fluidity of the mission environment. This would make the armed forces more mobile, more agile, less vulnerable, and less predictable (Royal Netherlands Army, 2018).

Related to the challenges and demands in future mission environments, the question remains how to conduct command and control in a complex, dynamic and networked mission environment. In the next section we discuss the challenges faced by the current hierarchical approach of command and control when operating in a complex, dynamic and networked mission environment.

1.3 Hierarchical approach to command and control: an impediment to mission effectiveness

The current conduct of command and control is based on hierarchal organisational structures, processes and procedures. However, hierarchical command and control is becoming an impediment to mission effectiveness in complex, dynamic and networked environments. Considering the demands of these environments, it is likely that the hierarchical approach of command and control will no longer meet the requirements of successfully performing operations. Several underlying reasons exists for this ineffectiveness (Van Bemmel et al., 2017):

- **Complexity and deep uncertainty of mission environments.** A traditional hierarchical approach to command and control is based on the idea that the world can be easily influenced, managed and shaped (by physical operations). However, this view on the world is not realistic with the current trends as described by the Land Warfare Centre (2015). Rather, contemporary conflicts are complex, multifaceted, and dynamic. Environments cannot be easily influenced, managed or shaped. The impediment of hierarchical command and control persists across all mission environments that are characterised by deep uncertainty and complexity, varying from megacities to rural areas;
- **Limited operational tempo and adaptivity because of time consuming decision-making.** The hierarchical approach to command and control limits operational tempo and the ability to be adaptive, mainly because the decision-making process is hierarchical and therefore not fast enough in relation to the demands of dynamic, networked environments;
- **More information in the field than on higher levels.** High (military) organisational levels often lack situational awareness and understanding to be able to command and control tactical operations aimed at achieving tactical effects, because in complex mission environments information is predominantly derived bottom-up, from the field;
- **Interaction and collaboration between military and civilian actors.** The mission environment in which future missions take place consists of a wide variety of both military and civilian actors who operate among and collaborate with the local population. Civilian actors cannot be commanded by the military; they can only be consulted or influenced. Interaction between military and civilian actors and harmonisation of efforts is needed to perform effectively in complex, dynamic and networked mission environments.
- **Limited possibilities of control.** The contemporary interpretation of control is based on the assumption that a mission environment can be controlled and managed. However, considering the complexity and dynamics of mission environments this is often not everywhere and always realistic.

In short, traditional hierarchical command and control is often too slow and ineffective in a complex, dynamic and networked environment with multiple diverse actors. Furthermore, hierarchical command and control often lowers the operational tempo, does not enhance adaptivity of military units and is not focused on harmonisation of military and civilian efforts. These challenges of a hierarchical approach of command and control are persistent across all mission environments and circumstances since deep uncertainty, high complexity and rapid change are part of the enduring nature of warfare.

1.4   What is NetForce?

NetForce is a paradigm of warfare for security and stability challenges in complex, dynamic and networked environments. NetForce builds on the theory of Network Centric Warfare (NCW) that was developed in the 1990s by the United States Department of Defence. The first complete articulation of the NCW approach can be found in the book Network Centric Warfare: Developing and Leveraging Information Superiority by David S. Alberts, John Garstka and Frederick Stein, published by the command and control Research Programme (CCRP) in 1999. Network Centric Warfare refers to a type of warfare that derives combat power from the networking of geographically dispersed forces, that have the ability, enabled by advanced information and communication technology, to share information and to create a high level of shared awareness, superior to that developed by an adversary. When exploited via self-synchronisation and collaboration that information advantage will lead to a competitive advantage and, in the end, mission success (Alberts et al, 1999). After the launch of the book Network Centric Warfare, many studies and experiments were carried out to explore and develop different elements and consequences of this type of warfare. Most of these studies and experiments focused on technological and interoperability challenges and less on challenges in the organisational and social domain.

Although NetForce builds on the ideas of Network Centric Warfare (NCW), it focusses specifically on topics in the organisational and social domain and not on the – albeit relevant – technological and interoperability challenges. The term NetForce was first introduced in a paper on Netforce principles (Keus, 2005). From a system of systems point of view Keus describes a NetForce as "the total collection of connected nodes that work together to perform a specific networked enabled capability." (Keus, 2005, p.2). Much later Van Dalen et al. (2017) describe NetForce as the total power that an adaptive (military) network can develop. According to Van Dalen et al. (2017), a NetForce may consist of military as well as civilian parties. We define NetForce as the total collection of connected civilian and military capabilities[4], interacting and collaborating with each other in an interorganisational, technical and social network.[5] These civilian and military capabilities share and work towards a high-level common objective in a complex, dynamic and networked mission environment (Van Bemmel et al, 2017). In short, NetForce refers to an (informal) coalition of civilian and military capabilities that strive for a similar high-level cause, for example reconstruction of an area after an earthquake, or safety and security in an area, conflict prevention, etc.

NetForce is defined as the total collection of connected civilian and military capabilities, interacting and collaborating with each other in an interorganisational, technical and social network. These civilian and military capabilities share and work towards a high-level common objective in a complex, dynamic and networked mission environment.

---

4.   A civilian or military capabilities are able to fulfil its function autonomously and can bring its intended effect in the mission environment.

5.   The definition is inspired by the paper on Netforce principles by Keus (2005).

Hence, a NetForce is not a formal organisation with clear tasks, roles, functions, processes, procedures and structures, but a fluid, temporary, and often ad hoc combination of military and civilian capabilities performing activities in a network. Personal objectives and interests of capabilities may vary from non-profit to profit or both. Depending on the context, the ratio between military and civilian capabilities in a NetForce may differ. In a context with a lot of violence, it is likely that the presence of military capabilities will have the upper hand. When the context becomes too violent, many civilian capabilities will leave because the area is too unsafe to operate. In a context of conflict prevention and reconstruction it is more likely that the presence of civilian capabilities will have the upper hand.

1.5   What is NetForce Command?

NetForce Command is a networked approach of command in which collaboration and information sharing are paramount and the function of command is (informally) shared with or distributed between capabilities contributing to a NetForce. Furthermore, the command relationships between these capabilities have a functional and informal character and not a formal character like in a hierarchical chain of command. This not only applies to relationships between and among civilian and military capabilities but also for capabilities from the same organisation e.g. the Netherlands Ministry of Defence. NetForce Command is developed to ensure that capabilities in complex, dynamic and networked environments will not be outdated, outpaced, outmanoeuvred and outsmarted. It is important to note that NetForce Command is not to replace a hierarchical approach of command and control. NetForce Command provides an alternative alongside the hierarchical approach of command and control and is specifically developed for complex, dynamic and networked environments, in which a high operational tempo, agility and harmonisation of effort are essential.

NetForce Command should meet the function and the principles of command and control for the armed forces. The function of command and control can be described as the function which enables the armed forces to direct and manage its efforts in order to reach its objective(s). According to the Netherlands Joint Doctrine Publication on Command and Control (Netherlands Ministry of Defence, 2012) the command and control function is based on the following four guiding principles:

1. Unity: the principle of unified leadership in order to reach unity of effort. Unity of effort aims to establish cohesion in the planning and execution of military operations designed to achieve a common goal (unity of purpose).
2. Continuity: the principle which says that a continuous process of activities in time and place must be assured throughout the entire duration of the operation or campaign.
3. Integration: the principle which argues that all components, supporting elements and capabilities which are contributing to the operation must be integrated in a joint structure in order to achieve the operational objectives.
4. Clarity: the principle which says that relationships must be properly established and that there is a need for clear delineation between the various roles and responsibilities in the chain.

NetForce Command can only be an effective alternative for a hierarchical approach of command and control, when it is capable of coping with the impediments of a hierarchical approach of command and control in complex, dynamic and networked mission environments as described in section 1.3. Therefore, we added the following principles for NetForce Command:

5. NetForce Command refers to functional, informal command relations in interorganisational, technical and social networks of military and civilian capabilities, not to formal command relations in a hierarchical (often military) chain of command;
6. NetForce Command is focused on maximising the power and influence of the connections and interactions of military and civilian capabilities in a network;
7. NetForce Command is focused on increasing operational tempo and adaptivity through empowerment (a high level of autonomy and freedom to act and decide, and in the extreme even the freedom to formulate own intent) of military and civilian capabilities in the complex, dynamic and networked mission environment;
8. NetForce Command envisions a supporting and facilitating role for the higher level (the parent organisations of military and civilian capabilities that contribute to a NetForce or NATO/UN headquarters), because in complex, dynamic and networked environments most information, situational awareness and understanding comes from the network, the NetForce.
9. NetForce Command is focused on harmonisation of the efforts of military and civilian capabilities by stimulating and strengthening networked interaction and collaboration between all capabilities, thereby unleashing the power and influence of a NetForce.
10. NetForce Command assumes that full control is (almost) impossible in complex, dynamic and networked mission environments and therefore uses an iterative or incremental approach to cope with challenges or to solve problems, whereas hierarchical command and control approaches often reason from an schematic, endstate driven approach.

These NetForce Command principles have several implications for the development of a NetForce Command concept. The principles, specifically the empowerment of military and civilian capabilities and the supporting role of the "higher level", imply that the NetForce Command concept should include a view on the organisation of command. The NetForce Command principles also imply that we need to rethink the implementation of the function of command and control, more specifically the three sub-functions leadership, decision-making and command. The current descriptions of the three sub-functions of command and control according to the Netherlands Joint Doctrine Publication on Command and Control (Netherlands Ministry of Defence, 2012)[6] are described below.

---

6. Within the current Netherlands Doctrine Publication (Netherlands Ministry of Defence, 2012), command consists of three elements leadership, decision-making, and command (bevelvoering). Within an international context command is often denoted as command and control (C2).

> 1. Leadership : the function which enables the purposely influencing of the behaviour of others in order to, by the use of own efforts, achieve the set objective.[7]
> 2. Decision-making: the function which enables the orientation, assessment and subsequent decision-making concerning various courses of action[8] in order to achieve the set objective in support of a higher (commander's) intent.
> 3. Command: the function which enables the organisation, direction and coordination of subordinate or supporting units, systems and/or platforms.

The principles of NetForce Command, specifically the emphasis on harmonisation by stimulating and strengthening networked interaction and collaboration to unleash the power and influence of NetForce, also require an extended view on collaboration and information management. In this regard the *attune* function is relevant to consider in relation to the command function. This *attune* function was recently added in the Netherlands future land operating concept (Land Warfare Centre, 2017), leading to six combat functions: *command*[9]*, shield, sense, affect, sustain and attune*.

> **Attune:** the function which enables all internal and external coordination and harmonisation efforts to generate all the capacity available.

To summarise, the NetForce Command principles imply that the development of a NetForce Command concept should include concepts for organisation, interaction and collaboration, command, leadership, decision-making and information management. In chapter 2 and 3 we elaborate on the NetForce concepts that were developed for these topics.

---

7. Currently a new Netherlands Joint Doctrine Publication on Command and Control is being developed. In this new doctrine a broader vision on leadership will be introduced. According to that vision the function of leadership will be focused on being a leader (character), doing (act, take initiative and adapt as leader, professional, coach, and/or manager) and learning ((self) reflection, development, training and innovation) leadership (Dalenberg et al, 2014) in order to develop a desired direction and/or to realise objectives.
8. Within the armed forces this function is usually implemented as a planning process.
9. Meaning command and control in an international context.

1.6   NetForce Command perspectives

The NetForce Command concept can be described from different perspectives. Because the NetForce Command concept is developed for the armed forces, we believe three perspectives are relevant from a military point of view: the perspective of the entire NetForce, the perspective of military capabilities contributing to NetForce and the perspective of the armed forces (an actor that contributes to the NetForce with military capabilities and functions as a parent organisation). These three perspectives are even more relevant, because the networked approach of command in the entire NetForce does not have to be similar to the networked approach of command in military capabilities or in the armed forces (as an actor that is contributing to NetForce with its capabilities). Furthermore, due to role differences the networked approach of command in military capabilities can differ from the networked approach of command in the armed forces.

Maximum
Self-synchronisation

Networked approach to
command and control

www.tno.nl/netforcecommand

NETFORCE COMMAND

FROM SELF-SYNCHRONISATION TO ORCHESTRATION

2

Maximum orchestration

Hierarchical approach to command and control

2 NETFORCE COMMAND FROM SELF-SYNCHRONISATION TO ORCHESTRATION

NetForce Command is a networked approach of command and control in which collaboration and information sharing between capabilities are paramount and the function of command is shared with or distributed between civilian and/or military capabilities contributing to a NetForce. Just as there are different implementations of a hierarchical approach of command and control, there are also different implementations of a networked approach of command and control – in other words different implementations of NetForce Command. All implementations of NetForce Command are focused on creating harmonisation of the efforts of military and civilian capabilities in a complex, dynamic mission environment and on increasing operational tempo and adaptivity. However, the implementations of NetForce Command differ in how harmonisation, a higher operational tempo, adaptivity and unity of effort come about.

The most extreme implementation of NetForce Command can be characterised as *self-synchronisation*. In NetForce, self-synchronisation refers to the ability of capabilities to synchronise their activities themselves, without being ordered to do so by another capacity.[10] There is no orchestrating power in the network. As illustrated in figure 3 capabilities may conduct activities together to achieve an effect and then part again in accordance with the self-perceived demands of the mission environment. Capabilities will strive for harmonisation with other capabilities that are conceptually or physically close to one another (e.g. that share a specific understanding of the mission environment), that want to contribute to the same issue in the mission environment, or that simply accidentally run into each other. This may lead to temporary sub-networks in which two or more capabilities collaborate. Successful self-synchronisation leads to a harmonisation of intents and efforts.
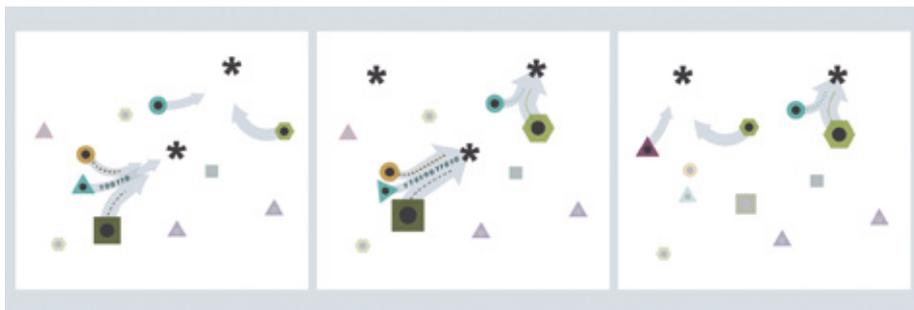
Figure 3 Self-synchronisation leading to harmonisation of intent and effort

---

10. There are many different definitions of self-synchronisation in a military context, e.g.: 'It is the ability of a well-informed force to organise and synchronise complex warfare activities from bottom up' (Cebrowski and Gartska, 1998) and 'It is the ability of a force to act in a manner coordinated in intent, time, and space with other battlespace entities, both civilian and military, without being ordered to do so specifically' (Gonzales, 2005).

In the mission environments in which self-synchronisation does not arise, is not desired or does not seem to work, different manifestations of orchestration may arise to support harmonisation, to increase operational tempo and adaptivity and to create unity of effort of the military and civilian capabilities in the NetForce.

The less extreme implementation of NetForce Command is one that can be characterised as *maximum orchestration*. Maximum orchestration in NetForce refers to an extreme form of harmonisation support provided by local and/or global elements. Harmonisation support is focused on creating unity of effort in a mission environment and is provided to military and civilian capabilities in the NetForce. The harmonisation support is provided and received based on mutual consent, which means there is no hierarchical relationship between the military and civilian capabilities that provide and receive harmonisation support. Because these relationships are functional and often informal, the civilian and military capabilities can decide not to accept and not to use the harmonisation support.[11] When the capability that provides orchestration does have the authority and responsibility to decide and to control, using orders and guidelines, there is no longer a networked approach to command and control (NetForce Command), but a hierarchical approach to command and control.

The different implementations of a networked and hierarchical approach to command and control can be visualised on a scale from maximum self-synchronisation to maximum hierarchical command and control. The scale is depicted in Figure 4. The different implementations of a networked approach to command and control (NetForce Command) refer to the left side of the scale: from maximum self-synchronisation to maximum orchestration. The different implementations of hierarchical command and control refer to the right side of the scale: from maximum orchestration to maximum hierarchical command and control. The implementation of command and control depends on the context, the actors that are contributing and the various and diverse capabilities. When these variables (context, actors and/or capabilities) change, the approach and implementation of command and control may change as well.

Figure 4: Different implementations of command and control on a scale from maximum self-synchronisation to maximum hierarchical command and control

---

11. However, there are circumstances in which military capabilities need (extreme) harmonisation support to align military activities and cannot afford to disregard the harmonisation support, for example to prevent risks like friendly fires incidents.

NetForce Command, and specifically terms like self-synchronisation and orchestration are not entirely new for the Royal Netherlands Army (RNLA). The Netherlands Doctrine Publication on land operations (Land Warfare Centre, 2014) describes a command philosophy built around the idea of a central intent and decentral realisation of that intent: "opdrachtgerichte commandovoering", also known as mission command. In the intent the "what" and "why" are emphasised in measurable effects and outcomes to be achieved, and the "how" is decided and performed in the field. Mission command provides mandate and stimulates freedom of action, unity of effort and initiative of lower level commanders. Mission command is focused on complex, dynamic environments, in which a high operational tempo, including rapid and timely decision-making, is essential. This command philosophy requires robustness (doctrine and core qualities) and agility to adapt command to the requirements of the environment. There are six principles of mission command:

1. unity of effort (= unity of thought + unity of purpose),
2. a main effort (which brings balance between unity of effort and freedom of action),
3. freedom of action in line with the intent (to respond adequately on changing circumstances and to synchronise activities),
4. trust,
5. mutual understanding and
6. timely and effective decision-making.

Mission command already allows for some level of self-synchronisation, but freedom is limited both by the elements that are predetermined by a higher level: intent, effort and main effort, and by time. One could argue that the NetForce Command scale from maximum self-synchronisation to maximum orchestration takes mission command to an unprecedented new level, where maximum self-synchronisation resembles self-command.

Different implementations of NetForce Command vary in the way harmonisation, a higher operational tempo, adaptivity and unity of effort come about. Depending on the composition, the organisation and structure, and the interaction in NetForce, the implementation of NetForce Command refers to another point on the scale from maximum self-synchronisation to maximum orchestration. These three aspects of NetForce are described in the next sections.

2.1 Composition of a NetForce

A NetForce is composed of different military and/or civilian nodes. Based on Keus (2005) a node is defined as a civilian or military capability that is able to fulfil its function autonomously, performs one or more activities in the mission environment and is able to interact with other nodes and other elements in NetForce.[12] A node may consist of one individual or a team trained and equipped to conduct certain tasks and achieve certain effects. A military node may for instance be an infantry company, a platoon or even a group, but probably not an individual soldier operating autonomously. A civilian node is for example a political advisor, a hacker, a UN employee or a unit of a construction company. Nodes can become part of a NetForce when their capabilities are contributory and they can leave a NetForce at any time, e.g. when their capabilities are no longer useful in the complex, dynamic mission environment. There are different types of nodes in NetForce:[13]

- **Effector nodes:** nodes that design, plan, execute and monitor activities to affect a mission environment and potentially elements outside the mission environment. Depending on the extent to which nodes are empowered by their parent organisation, they have more or less autonomy to decide what to do and how to act.
- **Supporter nodes:** nodes that design, plan, execute and monitor activities to provide support (for example logistical, judicial, infrastructural and medical) to all other nodes in NetForce.
- **Communicator nodes:** nodes that design, plan, execute and monitor activities to facilitate communication and information management between all other nodes in NetForce.
- **Sensing nodes:** nodes that design, plan, execute and monitor activities to direct, collect, process and disseminate information to all other nodes in NetForce.[14]

Most nodes represent a military or civilian actor. An actor refers to a joint, interagency, multinational or public (JIMP) organisation, for example a Ministry of Defence, an non-governmental organisation, a construction company, an embassy, etc. Military and civilian actors may contribute to a NetForce with one or more capabilities and function as their parent organisations. Note that in practice not each node necessarily has a parent organisation. In general, parent organisations support the deployment of their capabilities and may exert more or less influence on the activities of their capabilities in NetForce depending on their approach to command and control. Furthermore, parent organisations may set boundaries, constraints and restraints for their capabilities regarding, for example sustainment and rules of engagement. In some implementations of NetForce Command, parent organisations also provide representatives to a more overarching international organisation or entity like NATO or the UN.

---

12. A capability is a capacity (people and means) trained to execute certain activities and achieve intended effects (ability).
13. The type of nodes are inspired by the article on NetForce principles by Keus (2005), but further developed in the NetForce Command research programme. We combined the nodes for data collection (collector) and the nodes for information processing and provision (information provider) into sensing nodes. Furthermore we decided to disregard the nodes for decision-making (decider), because decision-making is part of all types of nodes.
14. The functioning of sensing nodes is part of the TNO research programme Sensing in a networked environment (SiaNE)

In NetForce two or more nodes may decide to collaborate in a temporary sub-network to achieve an objective and/or to perform a complex activity, for example the reconstruction of a road after a land slide. Each of the nodes that want to collaborate in a temporary sub-network will send one or more representatives and will provide a capacity that is needed to achieve that goal and/or perform that activity. For example, to reconstruct a road the following capabilities are needed: engineering, construction, security of the reconstruction site, provision of reconstruction material, communication with local population, and governance. The nodes (more specifically some representatives of the nodes) that provide these capabilities will collaborate in a temporary sub-network for the design, planning and execution of the activities that are needed to perform the complex activity. The collaboration in a temporary sub-network is temporary in the sense that the collaboration will end or change when the objective of the temporary sub-network is reached. In practice the collaboration may take a few days up to a few months or even a year. A temporary sub-network is only formed when two or more nodes decide to collaborate, not when they only want to deconflict or coordinate. The character of a temporary sub-network is determined by its function, composition, culture, structure, organisation and behaviour.

In the mission environments in which self-synchronisation is not possible or desired, orchestration arises to support harmonisation and to create unity of effort amongst civilian and military nodes. In those cases orchestrating elements are formed. This may be initiated from the bottom up (by a temporary sub-network or by military and civilian nodes) or from the top down (by parent organisations). Orchestrating elements support harmonisation and create unity of effort amongst military and civilian nodes in NetForce by creating shared situational understanding and by providing harmonisation support for the design, planning, and attunement and alignment of activities in order to realise desired effects in the mission environment. In other words, orchestrating elements may provide synchronisation of the processes and activities of civilian and military nodes in NetForce in the following ways:

- By supporting shared situational understanding that is conditional for harmonisation (*shared situational understanding*),
- By supporting the harmonisation process of developing a dynamic design and translating that design into activities *(design)*,
- By supporting the harmonisation process of determining how to use military and civilian capabilities (the means) and by determining whom in time and space is to realise the objective(s) *(planning)*, and
- By supporting the harmonisation process of coordinating the execution of activities by military and civilian nodes to realise objective(s) *(attunement and alignment)*.

It is expected that orchestrating elements formed by parent organisations will try to exert more guiding influence than orchestrating elements that are formed by temporary sub-networks or the nodes. The way an orchestrating element is formed, influences its function, composition, culture, structure, organisation and its style of orchestrating.

To increase their influence on the NetForce military and civilian actors can decide not only to contribute to the NetForce with one or more capabilities, but also to participate in a strategic coalition. A strategic coalition is not physically present in a mission environment where the crisis or mission takes place. A strategic coalition consists of political strategic representatives of different actors (JIMP organisations) who may also contribute to the NetForce with capabilities. A strategic coalition for specific mission environments can also be formed by overarching organisations like UN, EU or NATO. The aim of a strategic coalition is to have orchestrating influence on the nodes, temporary sub-networks and orchestrating elements in a NetForce. This orchestrating influence is more or less guaranteed by its size, position and scope. In practice it will therefore be hard for the elements in the NetForce to ignore the orchestrating influence of a strategic coalition. A strategic coalition may try to exert orchestrating influence in different ways, including: providing support, information and state-of-the-art technology, networking with other actors, forming of an orchestrating element, influencing via the orchestrating elements, influencing the nodes and temporary sub-networks directly, etc. The way a strategic coalition is formed influences its function, composition, culture, structure, organisation and its style of operating.

Nodes   Parent organisations   Temporary sub-networks   Orchestrating elements   Strategic coalitions

Figure 5 Overview of elements in NetForce.

Maximum
Self-synchronisation

Networked approach to
command and control

Maximum
orchestration

Hierarchical approach to
command and control

Watch the explanimation Envisioning NetForce
www.tno.nl/netforcecommand

2.2   Organisation and Structure of Command in a NetForce

There are infinite implementations of NetForce Command on the scale from maximum self-synchronisation to maximum orchestration. They differ in how harmonisation comes about and how unity of effort is created in NetForce. To illustrate some of the potential implementations of NetForce Command we chose three distinct points on this scale from maximum self-synchronisation to maximum orchestration. The main difference between these three implementations concerns the organisation and structure of NetForce Command. We refer to these three distinct implementations of NetForce Command as:

• Archetype A: Emergent NetForce
• Archetype B: Emergent Orchestrated NetForce
• Archetype C: Strategic Orchestrated NetForce

Archetype A is the most extreme implementation of NetForce Command, as the maximum level of empowerment of nodes, distribution of information and the existence of informal organisational structures is reached. Archetype C is an implementation of NetForce Command on the other end of the scale, towards maximum orchestration. Archetype B is positioned approximately halfway between A and C on the scale. As Archetype A, B and C are potential implementations of NetForce Command on a continuum (see Figure 4) the exact boundaries are not specifically defined. Moreover, there is no optimal archetype. Depending on the context, mission type, phase of conflict, actors and capabilities involved one archetype is more suitable than the other. In the remainder of this section the three archetypes are introduced and explained in more detail (Van Bemmel et al., 2017).

Archetype A: Emergent NetForce

Archetype A, as depicted in Figure 6, is a NetForce Command implementation in which a NetForce emerges out of activities of different civilian and military nodes who are all committed to a common objective in a certain complex, dynamic mission environment, for example reconstruction of an area after an earthquake, or safety and security in an area, conflict prevention, etc.
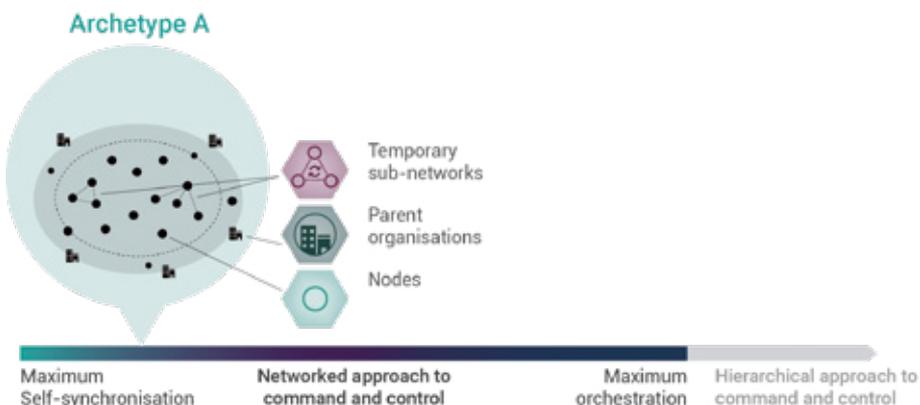

Figure 6 Illustration of NetForce archetype A

Military and civilian actors may contribute to a NetForce with one or more nodes and function as their parent organisations. It is also possible that a node functions without a parent organisation, for example volunteers with specific skills and idealistic motives like teachers or hackers. Furthermore, in the surroundings of the NetForce you may find actors that choose not to be part of the NetForce explicitly. These actors may be neutral, supportive or unsupportive towards the intention or high-level objective(s) of the NetForce. In principle, the network has a fluid structure, which means that actors can decide at any times to leave the NetForce or to become part of it.

In archetype A the civilian and military nodes operate by self-synchronising their activities; they harmonise their activities and create unity of effort amongst one another. In general, the nodes may be influenced or consulted, but not commanded or controlled by any one of the other nodes. Furthermore, there is no orchestrating element or strategic coalition that provides harmonisation support or contributes to unity of effort.

In archetype A developments in the mission environment may give rise to temporary sub-networks in which two or more nodes collaborate and self-synchronise for a complex activity. In these sub-networks temporary hierarchical command structures are still possible at local level, for example to plan and execute a combat action. The sub-networks have their own objective, often related to the overall objective of the NetForce. A sub-network dissolves when its objective is realised or when the situation or context changes and the sub-network is no longer relevant.

Archetype B: Emergent Orchestrated NetForce

Archetype B, as depicted in Figure 7, distinguishes itself from Archetype A by the arising need for orchestration of activities of the civilian and military nodes. Between archetype B and the far right side of the scale, orchestrating elements are formed to contribute to shared situational understanding and to provide harmonisation support for the designing, planning, attuning and alignment of activities of civilian and military nodes in order to realise desired effects in the mission environment.
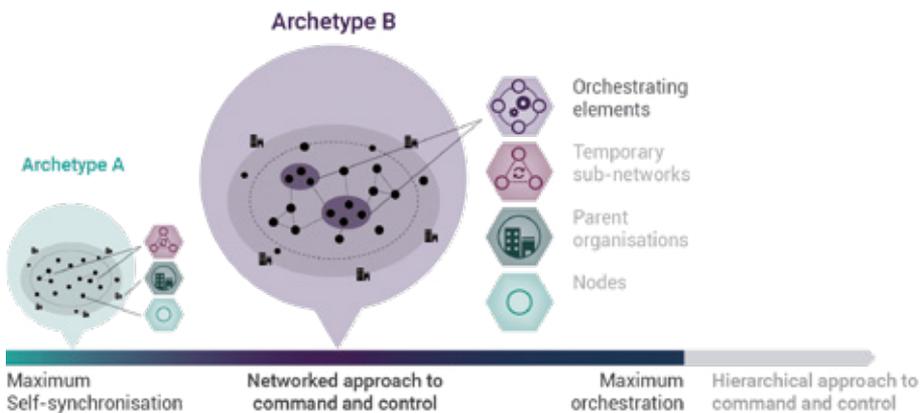

Figure 7 Illustration of NetForce archetype B

There are different views on where the decision to form orchestrating elements is made. On the one hand, the orchestrating elements may emerge bottom-up (from what starts as a temporary sub-network) and will provide harmonisation support when there occurs a need within the NetForce. On the other hand, the orchestrating elements may be designed by the parent organisations or the overarching organisations and provide harmonisation support and guidance from the start. One might argue that these two variants represent two different NetForce archetypes. We chose to incorporate both in archetype B, but both variants represent a slightly different point on the NetForce Command scale from maximum self-synchronisation to maximum orchestration, represented in Figure 4. It is expected that in the latter variant, the orchestrating elements will have more of a guiding influence and some decision rights may even be allocated to the orchestrating elements. However, when the nodes are in agreement, an orchestrating element that is developed from the bottom up may also have decision rights. Depending on the mission environment and the needs of the NetForce one or more orchestrating elements may be formed. The orchestrating elements can disassemble themselves and/or change their function and purpose when the needs of the NetForce change. However, it is expected that, in contrast with temporary sub-networks, orchestrating elements will often be required for a longer period of time.

Archetype C: Strategic Orchestrated NetForce

Archetype C, as depicted in Figure 8, is a NetForce variant that differs from archetype A and B in the sense that the NetForce is supported and influenced by a coalition on political strategic level: a strategic coalition. A strategic coalition for specific mission environments consists of political strategic representatives of different actors, JIMP organisations, that also contribute to the NetForce with capabilities, and can also be formed by overarching organisations like UN, EU or NATO. Between archetype C and the far right side of the scale a strategic coalition can have orchestrating influence on the nodes, temporary sub-networks and orchestrating elements in a NetForce in different ways, including: providing support, information and state-of-the-art technology, networking with other actors, forming of an orchestrating element, influencing via the orchestrating elements, influencing the nodes and temporary sub-networks directly, etc.
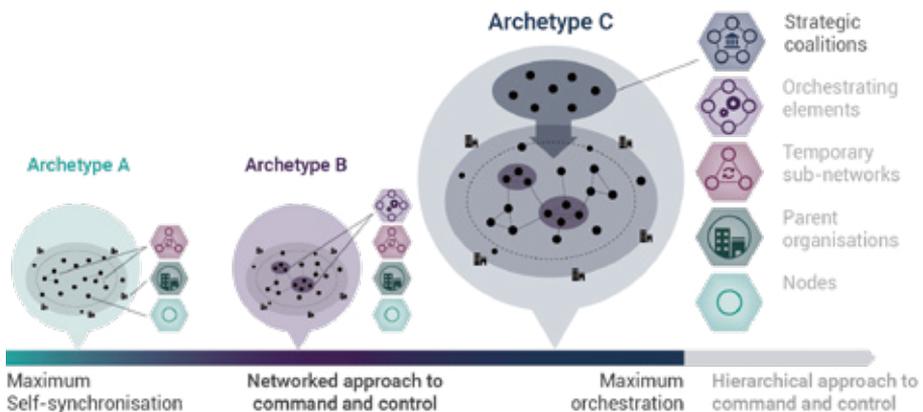

Figure 8 Illustration of NetForce archetype C

Because of the political strategic level and the position of a strategic coalition, it is likely that it will exert influence and play a leading role in the NetForce, directly or indirectly via the orchestrating elements. In archetype C the role of the orchestrating elements may be formalised more due to the influence of the strategic coalition. They will have more of a guiding influence in this archetype than in archetype B. Furthermore, archetype C creates challenges for the nodes and the temporary sub-networks. With orchestrating elements and a strategic coalition, full self-synchronisation of the nodes as described for archetype A is no longer self-evident.
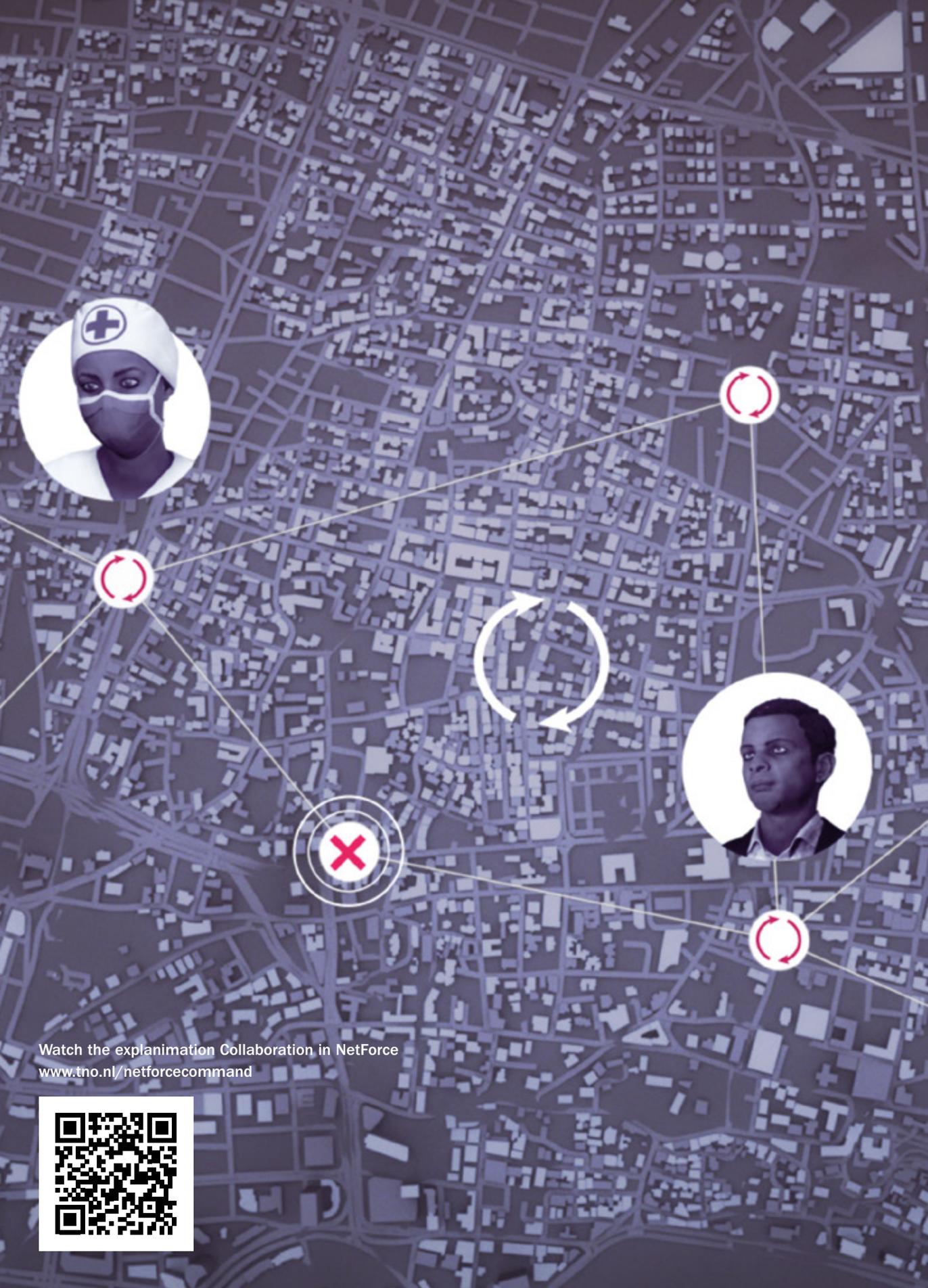
2.3   Interaction in NetForce

The process of harmonisation and achieving unity of effort in a NetForce depends on the composition, the organisation and structure of NetForce Command, but also on the interaction of the different elements in NetForce: nodes, temporary sub-networks, orchestrating elements, and strategic coalitions.

Need for interaction

The need for some level of interaction is determined by the gap between the abilities to realise objectives and the requirements of the mission environment. When elements in NetForce lack the abilities for realising objectives in the mission environment, the need for some level of interaction arises. This need can arise from the bottom up or from the top down:

1. From the bottom up: the nodes, temporary sub-networks and orchestrating elements in NetForce feel the need to interact and collaborate to be able to realise objectives in the mission environment.
2. From the top down: parent organisations or a strategic coalition decide to stimulate, facilitate or even enforce interaction between nodes, temporary sub-networks and orchestrating elements to become more successful in the mission environment.
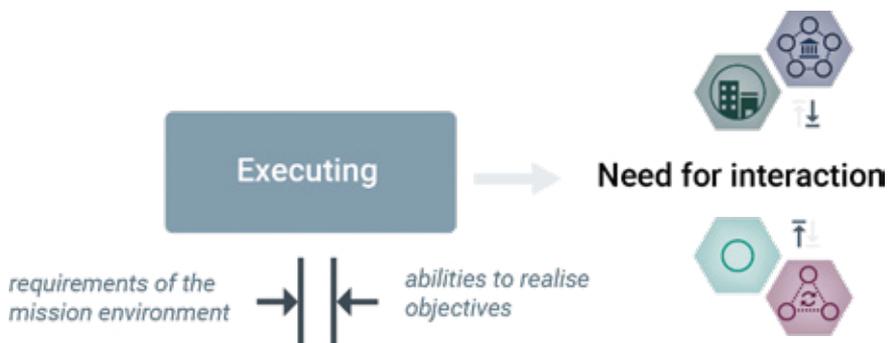

Figure 9 Gap from which the need for interaction arises

Types and levels of interaction in NetForce

The elements in NetForce may have several reasons for interaction. In complex, dynamic and networked mission environments some level of interaction with complementary partners is often a necessity to realise an element's own and the network's common objectives. In NetForce several types of interactions are possible:

• A node interacts with its own parent organisation and may interact with one or more other nodes and/or with temporary sub-networks, orchestrating elements, and strategic coalitions of which it is not part;
• Representatives of nodes interact in temporary sub-networks;
• Temporary sub-networks may interact with nodes, other temporary sub-networks, orchestrating elements and/or strategic coalitions;
• Representatives of nodes interact in orchestrating elements;
• Orchestrating elements may interact with nodes, temporary sub-networks, other orchestrating elements and/or strategic coalitions;

- Representatives of actors/parent organisations interact in strategic coalitions;
- Strategic coalitions may interact with nodes, temporary sub-networks, orchestrating elements and when present also with other strategic coalitions;
- Actors (parent organisations) interact with their own nodes and may interact with other actors (parent organisations), strategic coalitions and sometimes also with orchestrating elements and temporary sub-networks, especially when representatives of their nodes are part of the orchestrating elements and temporary sub-networks and when they stimulated the forming of these elements.

		Nodes	Temporary sub-networks	Orchestrating elements	Strategic coalitions	Parent organisations
Nodes	interact with					
Representatives of nodes	interact in					
Temporary sub-networks	interact with					
Orchestrating elements	interact with					
Strategic coalitions	interact with					
Parent organisations	interact with					
Representatives of parent organisations	interact in					

Figure 10 Type of interactions between elements in NetForce

The level of interaction can differ from unawareness to awareness, deconfliction, coordination, collaboration and even integration. These levels of interaction are described by NATO SAS 143 Research Task Group and depicted and explained in figure 11.
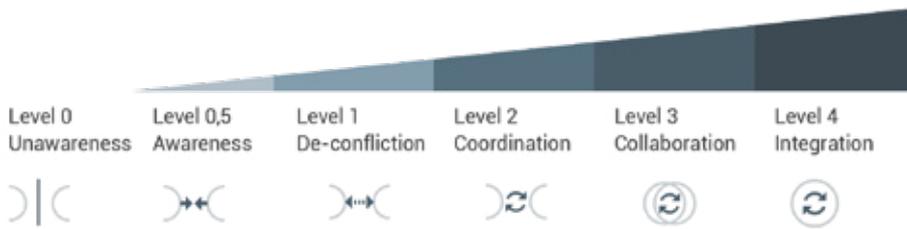
Figure 11 Levels of interaction scale

	Level 0 Unawareness	–
	Level 0,5 - Awareness	Without direct interaction, elements in NetForce need to be aware of each other, recognise potential conflicts and adjust as they think necessary.
	Level 1 - Deconfliction	Elements in NetForce interact as necessary to recognise and understand potential conflicts, agree to avoid them, and constrain their behaviour.
	Level 2 - Coordination	Elements in NetForce interact as necessary to recognise and develop a degree of mutual intent and agree to shape and adjust their plans and operations.
	Level 3 - Collaboration	Elements in NetForce interact as necessary to develop a collective intent and both a partially integrated plan and operations to achieve synergies.
	Level 4 - Integration	Elements in NetForce integrate themselves to create and act as one 'new' element.

The level of interaction depends on the need and objective of the interaction. When it is important to know of each other's presence in a mission environment, the interaction does not need to exceed the level of awareness. When, for example, a node needs to ensure that its activities are not hampering the activities of another node, a higher level of interaction is needed (deconfliction or even coordination). When, for example, two or more nodes decide to form a temporary sub-network to perform an activity and to realise an objective, an even higher level of interaction is required. In that case the purpose of the interaction between the nodes requires the level of collaboration or even integration. The higher levels of interaction (Collaboration or Integration) apply to functioning NetForce collaborations like temporary sub-networks, orchestrating elements and strategic coalitions.

Multiple ties

Each element in NetForce has multiple connections (multiple ties) with other elements in NetForce. Via those ties each element in NetForce influences the functioning of other elements in NetForce. Multiple ties can become challenging for the higher levels of interaction, collaboration and integration when they are conflicting, but also for the lower levels of interaction when they decrease autonomy and hamper self-synchronisation. In NetForce, five types of ties can be distinguished:

1. **Authority ties:** the formal influence of parent organisations on their nodes, the representatives in temporary sub-networks, the representatives in orchestrating elements and the representatives in strategic coalitions;

2. **Mutual influence ties:** the influence of the nodes on each other, the influence of temporary sub-networks on each other, the influence of orchestrating elements on each other, the influence of strategic coalitions on each other, and the influence of parent organisations on each other.

3. **Network influence ties:** the influence of temporary sub-network on independent nodes;

4. **Orchestration ties:** the influence of orchestration elements on the nodes and the temporary sub-networks;

5. **Strategic influence ties:** The influence of strategic coalitions on the nodes, temporary sub-networks, and orchestrating elements.

In NetForce Command archetype A there are three types of ties that have influence: 1) authority ties, 2) mutual influence ties, and 3) network influence ties. In archetype B a fourth type of ties becomes influential: 4) the orchestration ties. Furthermore, the influence of the authority ties is broadened to the representatives of actors/parent organisations in orchestrating elements. In archetype C a fifth type of ties is influential: 5) strategic influence ties. And the influence of the authority ties now also includes the representatives of actors/parent organisations in the strategic coalitions. Note that in archetype C the nodes have to deal with five different types of ties, whilst in archetype B and A the nodes have to deal with respectively four or three types of ties. In general, the more ties a node has to deal with, the more challenging and complicated its autonomous functioning becomes.[15] An overview of the types of ties per archetype is depicted in Figure 12.
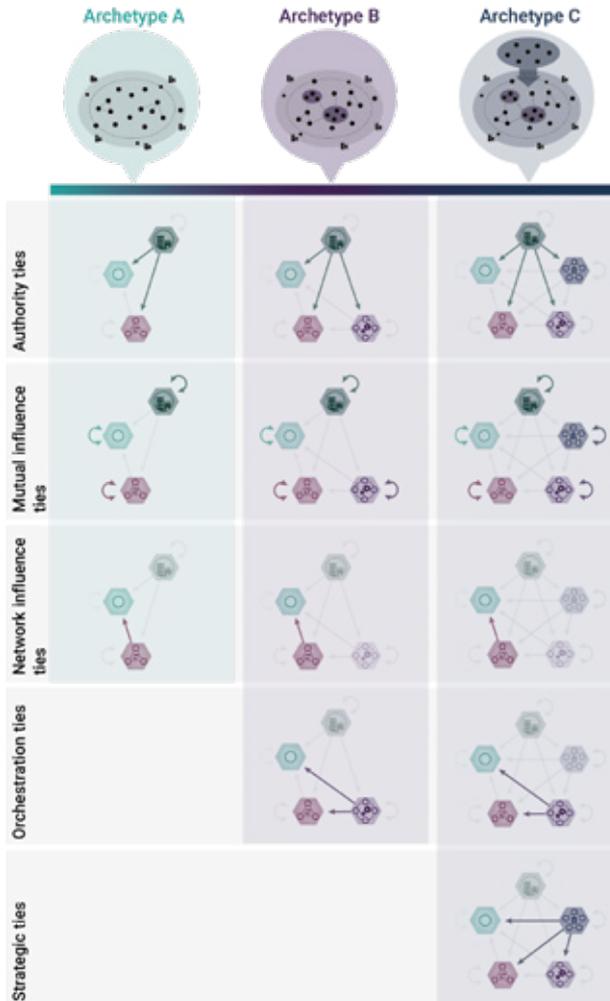
Figure 12 Overview of influence ties

---

15. Although not directly relevant for NetForce, it is worth noting that in contemporary missions like NATO ISAF there often were two authority ties: the formal influence from the parent organisation on the nodes and the formal influence of the international organisation (NATO, EU, UN) that performs the mission to which the parent organisation contributes. This makes contemporary military missions very challenging, especially when these two authority ties are conflicting ones.

Phases of interaction and collaboration

In complex, dynamic and networked mission environments interaction between different actors, and often collaboration or even integration, are a necessity to achieve objectives. However, it is difficult to develop interaction, especially collaboration or integration, in ad hoc relationships with various actors. Differences in organisational cultures, backgrounds and capabilities, for instance, form a reason to collaborate, but also create potential tensions and risks (Kalkman, Kerstholt & Roelofs, 2018).

An interaction may manifest itself in different phases of ad hoc interaction and collaboration. In previous TNO research four teambuilding models were studied (Tuckman, 1965, Tjemkes et al., 2012, Rietjens, 2008 and Ring & Van de Ven, 1994) for the development of an intelligent Collaboration Building Suite (iCOBUS) that supports collaboration building in ad hoc circumstances (Kamphuis et al., 2014; Eikelboom et al., 2016). These four models were integrated into one model that suits ad-hoc interactions and collaborations in mission environments. In that model, interactions go through four phases: positioning, shaping, executing and transforming (Kamphuis et al., 2014). Because interaction and collaboration in NetForce will often have a temporary and ad hoc character, the model is very applicable to NetForce.

Figure 13 Summary of process model for interaction in NetForce

Each of the four phases has its unique goals, activities, decisions, challenges and tensions. The interaction between elements in NetForce can jump back and forth in phase, for example when something changes in the partner constellation (e.g. a new node is added) or when the objective or the interests of one or more partners change. The four phases of ad hoc interaction and collaboration are described below (Kamphuis et al., 2014):

- **Positioning phase:** in the positioning phase an element in NetForce determines its own position in comparison to the other elements. Relevant partners are identified and the terms of possible collaborations are discussed based on an initial idea about the function and purpose of collaboration(s). The positioning phase results in decisions about with whom only co-existence or awareness is desired, with whom deconfliction and/or coordination is sufficient and possible and with whom collaboration or even integration is needed and desired. There are multiple reasons for collaboration or even integration in temporary sub-networks. These reasons are amongst others: to improve situational understanding, to have more impact, to block competitors/opponents, to have access to resources/capabilities, to enhance economics of scale, to share risks or costs, to improve reputation, to learn from each other or to share knowledge. Communicating the reasons for collaboration is important and can enhance an effective and successful collaboration, especially when there are conflicting reasons and objectives.
- **Shaping phase:** in this phase the desired level of interaction is formed via a partly conscious and unconscious group dynamic process of social interaction between (representatives of) nodes. Awareness does not need any shaping. Deconfliction and coordination need some harmonisation effort (attuning) on potential differences in for example communication and organisation. Collaboration and integration need more harmonisation effort: more detailed agreements about the function and purpose of the collaboration or integration (initially discussed in the positioning phase) and more shaping of the collaboration in terms of composition, organisation & structure, culture and group behaviour. These four characteristics are inspired by the framework of Whelan (2015)[16] about networked collaboration and described in Roelofs et al. (2017). To be able to identify different manifestations of a collaboration, the key variables (including their underlying indicators) are combined into a NetForce Collaboration Framework. The NetForce Collaboration Framework is included in annex B.
The emergence of group behaviour includes behaviour related to management and control (see section 3.1 and 3.2), leadership and followership (see section 3.3), decision-making (see section 3.4), and information sharing (see section 3.5).
- **Executing phase:** in the executing phase the different elements in NetForce design, plan, execute and monitor their activities or operations, depending on the agreements related to management and control, leadership, decision-making and information sharing, that are made in the shaping phase. Depending on the function, purpose and objectives, an element in NetForce will have different levels of interaction with other elements. In the execution phase all kinds of internal and external factors may influence the group dynamics and consequently the effectiveness and efficiency of the interaction. Examples of internal factors that influence the group dynamics are trust between the elements that interact, motivation to share information with each other, and the (potentially conflicting) own interests of each element in the interaction. Examples of external factors that influence the group dynamics are events in the mission environment and new collaborations that arise in the immediate vicinity of an element in NetForce.

---

16. Whelan's framework (2015) consists of the following elements that should be considered by organisations that are in the transition to a networked form of collaboration: 1) network structure, 2) network culture, 3) network policy; 4) network relationships; and 5) network technology.

- **Transforming phase:** in the final phase, the transforming phase, the interaction comes to an end or transforms into another interaction. There are different internal and external triggers that start the transforming phase. Examples of internal triggers are: one or more participants in the interaction are dissatisfied about the amount of progress in realising individual and/or common objectives, or participants are not satisfied with the interaction (e.g. information exchange, coordination, decision-making), or objectives and interests are changing. External triggers can also lead to transformation, for example a change of policy by one of the actors or changes in the mission environment (e.g. politics, challenges). In a transforming phase, the function, composition, organisation and structure, culture and functioning of an interaction may change and lead to the forming of a new interaction or to the dissolvement of the interaction. When a new interaction is desired, the shaping phase is repeated.

In the model on the next page (Figure 14) the dynamics of these four phases of interaction and collaboration are illustrated.

2.4   Concluding remarks

The different potential implementations of NetForce Command on the scale from maximum self-synchronisation to maximum orchestration, and more specifically the possible compositions, organisations and structures, and interactions in NetForce that determine those different potential implementations of NetForce Command, become more tangible in chapter 4, which consists of interviews with future actors and provides an impression of NetForce Command in the three archetypes that were presented in this chapter. The different potential implementations of NetForce Command on the scale from maximum self-synchronisation to maximum orchestration, including the possible compositions, organisations and structures, and interactions have implications for military nodes and the armed forces in general. In chapter 6 we provide a broad overview and analysis of implications of NetForce Command along the DOTMLPFI[17] lines, which are essential factors for developing and implementing the capability NetForce Command. More information on the elements in NetForce, the NetForce archetypes, and the emergence of interactions in NetForce can be found in the further reading suggestions below.

---

17. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
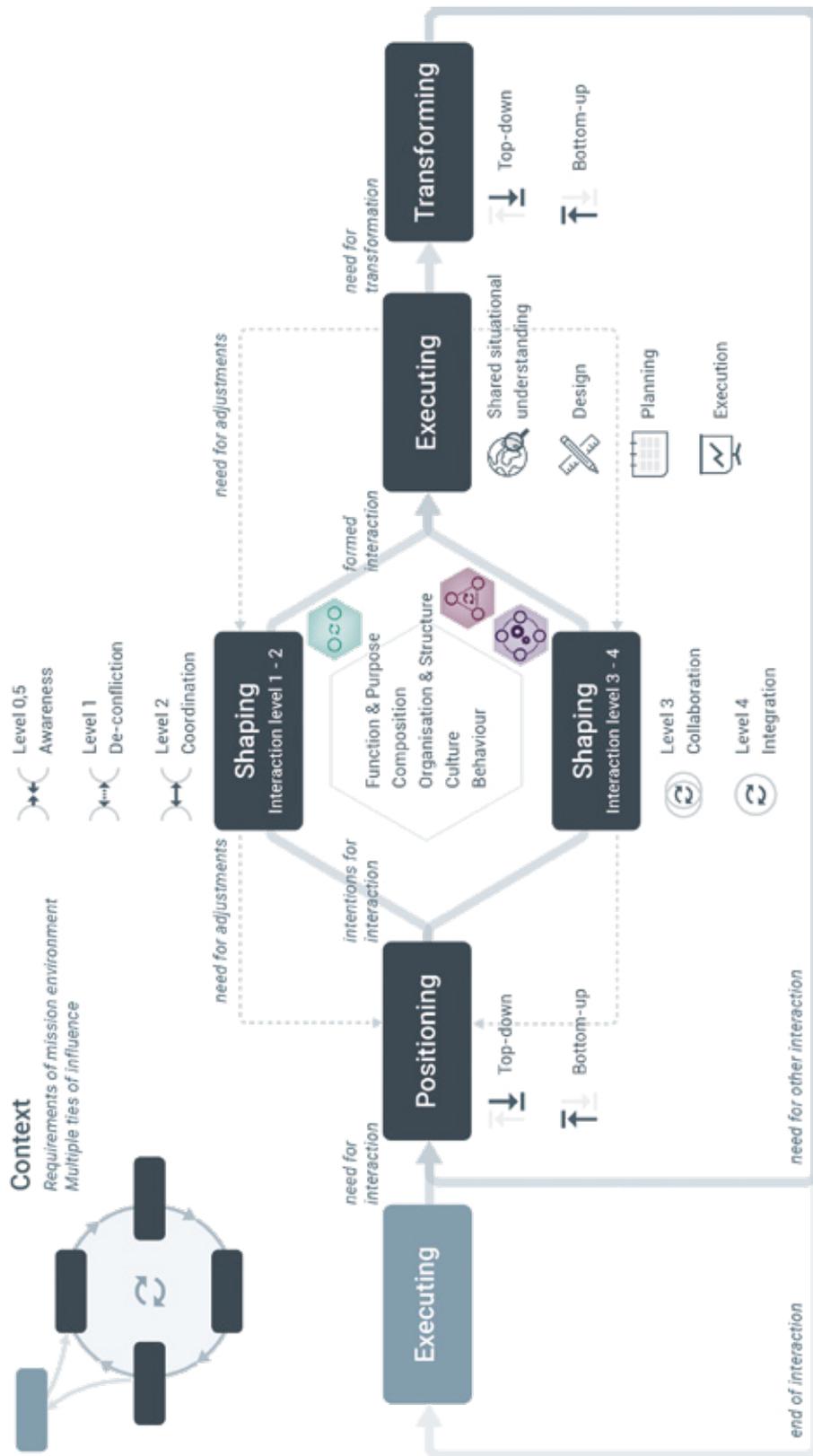
Figure 14 Process model for interaction in NetForce

Further reading

Bemmel, I.E. van, Eikelboom, A.R., Hekken, M.C. van, Benda, R., Roelofs, M,L., Pieneman, R., & Kuijt, J.T. van de (2017). NetForce Command, the next step?!. Paper presented at 22nd International Command and Control Research and Technology Symposium (ICCRTS) 2017, 6-8 November, Los Angeles, California (USA). http://internationalc2institute.org/proceedings.

Roelofs, M.L., Kerstholt, J., & van Bemmel, I.E. (2017). Networked collaboration: lessons learned from the civilian domain. Paper presented at 22nd International Command and Control Research and Technology Symposium (ICCRTS) 2017, 6-8 November, Los Angeles, California (USA). http://internationalc2institute.org/proceedings.

Roelofs, M.L., Bemmel, I.E. van, Kalkman, J.P. & Kerstholt, J.H. (2018). The influence of multiple ties on networked collaboration and decision-making. TNO report: TNO 2018 R10563, Soesterberg: TNO.

Roelofs, M.L., Hekken, M.C. & Vos, P.M. (2019). V1604 NetForce Collaboration – characteristics of collaboration in temporary sub-networks. TNO report: TNO 2018 R11415, Soesterberg: TNO.

NETFORCE
COMMAND
CONCEPTS

3

3 NETFORCE COMMAND CONCEPTS

In complex, dynamic and networked mission environments interaction between different actors, and often collaboration or even integration, are needed to realise effects. However, it is difficult to develop interaction, especially collaboration or integration, in ad hoc relationships with various actors. In section 2.3 we introduced the four development phases of ad hoc interaction and collaboration: positioning, shaping, executing and transforming (Kamphuis et al, 2014). Each of the four phases has its unique goals, activities, decisions, challenges and tensions. The interaction between elements in NetForce can jump back and forth in these four phases, for example when a new node joins the NetForce or when the interests of partners change.

In the positioning phase each element in NetForce (i.e., nodes, temporary sub-network, orchestrating element or strategic coalition, see section 2.1) determines his own position in comparison to the other elements in NetForce. The positioning phase results in decisions about with whom to co-exist, deconflict, coordinate, collaborate or even integrate. In the shaping phase the chosen level of interaction is formed in the group dynamics that result from social interaction between two or more nodes. Group dynamics refer to behaviours and socio-psychological processes within a social group or between social groups. Group dynamics are influenced by the behaviours and characteristics of the actors involved (nodes and parent organisations), the events and developments in the mission environment and the type of mission. Depending on the group dynamics, the interaction between nodes will develop differently in terms of group behaviour. Furthermore, depending on the group dynamics the collaboration between (representatives of) nodes in temporary sub-networks, orchestrating elements and strategic coalitions will be shaped differently in terms of composition, organisation and structure, culture and group behaviour. This means that there are infinite manifestations of interactions and collaborations in NetForce.

Aspects of the emerging group behaviour in the interaction between nodes and in the collaboration between (representatives of) nodes in temporary sub-networks and orchestrating elements and strategic coalitions pertain to management and control, leadership and followership, decision-making, and information management. In this chapter we describe how these aspects of group behaviour in NetForce Command are formed in the shaping phase: self-synchronisation (section 3.1), different levels of orchestration by orchestrating elements (section 3.2), leadership (section 3.3), decision-making (section 3.4) and information management (section 3.5).

3.1 Self-synchronisation

In chapter 2 we introduced NetForce Command as a networked approach of command and control in which collaboration and information sharing between capabilities are paramount and the function of command is shared with or distributed between civilian and/or military capabilities contributing to a NetForce. There are different implementations of a networked approach of command and control, or, in other words, there are different implementations of NetForce Command. The most extreme implementation of NetForce Command can be characterised as self-synchronisation. Self-synchronisation is described by Albert and Hayes (2003) as the operating of entities in the absence of traditional hierarchical mechanisms for command and control. According to Gonzales (2005): 'Self-synchronization is the ability of a force to act in a manner coordinated in intent, time, and space with other battlespace entities, both civilian and military, without being ordered to do so specifically.' In this book, we adopt the definition of Cebrowski and Gartska (1998) on self-synchronisation and apply it to a network of nodes instead of a force: 'It is the ability of a well-informed force to organise and synchronise complex warfare activities from bottom up.'

> "It is the ability of a well-informed force to organise and synchronise complex warfare activities from bottom up."

According to Cebrowski and Gartska (1998), shared situational awareness and a common rule set are two of the key elements of self-synchronisation. NetForce operations, however, take place in complex mission environments with multiple military and civilian nodes with different beliefs, cultures and values. In such an environment, it is almost impossible to create shared situational awareness and a common rule set. Although we do acknowledge that the creation of situational awareness is important and that it is significant to have shared intentions, we believe shared situational awareness and a common rule set are not strictly essential nor attainable. We believe that nodes that are able to take perspective or accept another node's point of view and understanding, can already engage in effective self-synchronisation. In other words, not all information necessarily needs to be shared and understood between the nodes, but the ability to freely distribute and share information among nodes is essential.

Challenges of self-synchronisation in NetForce

In the most extreme implementation of NetForce Command, the function of command and control and related decision authority is implemented at field level with empowered nodes who operate and synchronise with other nodes in NetForce. Self-synchronising nodes may be influenced or consulted, but not commanded or controlled by any one of the other nodes. There is also no orchestrating power in the network to support them. Nodes may aggregate – conduct activities or bring effects together – and disaggregate in accordance with the self-perceived demands of operational reality. Nodes will strive for harmonisation with other capabilities that are conceptually or physically nearby, for example those who share a specific understanding of the mission environment, that want to contribute to the same issue in the mission environment or that accidentally run into each other. This may lead to temporary sub-networks in which two or more nodes collaborate. Successful self-synchronisation leads to a harmonisation of intents and efforts.

"In the most extreme implementation of NetForce Command, the function of command and control and related decision authority is implemented at field level with empowered nodes who operate and synchronise with other nodes in NetForce."

Achieving and conducting a self-synchronisation approach to command and control will be challenging. With regard to the coordination between nodes and the execution of activities these challenges relate to communication, self-sufficiency, virtual collaboration, team cohesion and trust. In the fluid network of collaborating nodes self-synchronisation may be different for each situation and can change over time. Establishing ad hoc partnerships, changing functional command relationships, shared and distributed leadership, and even civilian leadership of military nodes will challenge self-synchronisation. How will self-synchronising nodes be able to harmonise their activities and conduct operations in a coherent way? What will enable nodes to conduct self-synchronisation? What does it mean for nodes to be empowered and to operate in a self-synchronising manner? Will the traditional function and principles of command and control as described in section 1.5 still stand when nodes operate in a self-synchronised manner and thus when the function of command and control is performed by the nodes in the field?

To understand self-synchronisation and to be able to draw implications for the armed forces when implementing self-synchronisation we take a pragmatic approach. By describing the process of self-synchronisation we are able to explore the implementation of the function of command and control at field level and may identify essential requirements for self-synchronising nodes. We therefore look at self-synchronisation as the process that includes four loops: understand, prioritise, harmonise and execute. These loops represent a distinct, but not isolated element of self-synchronisation and influence each other continuously. For example the understand loop, in which amongst others situation awareness is created, is heavily influenced by harmonisation efforts with other nodes and the execution of activities.

"We look at self-synchronisation as the process that includes four loops: understand, prioritise, harmonise and execute."

Process of self-synchronisation

Within the Multinational Capability Development Campaign (MCDC) Information Age Command And Control project (2017 and 2018), self-synchronisation is described as a process with the loops understand, prioritise, harmonise and execute as depicted in Figure 15. These loops were chosen as they each represent a distinct, but not isolated element of self-synchronisation. They are in continuous interaction with each other and influence each other's progress. The level of understand, prioritise, harmonise and execute will need to be sufficient, depending on the intended and/or current activity and the mission environment, to result in effective self-synchronisation.

Understand and prioritise are described as 'node internal' loops, as the functions in these loops are described as node internal processes (processes each node will go through individually). Of course, in effective self-synchronisation, none of these loops is run in splendid isolation by a single node. Though the outcomes of these 'node internal' loops can be specific for each node, these loops also benefit from and build on information exchange and interaction between nodes. However, the (process of) communication the nodes have regarding their understanding and prioritisation is described as part of the harmonisation loop. The harmonise and execution loops have an external focus and describe the interaction between at least two nodes. Nodes harmonise their priorities or responses with requests of other nodes; by doing so they reassess their priorities, reverting to their internally focused loops.
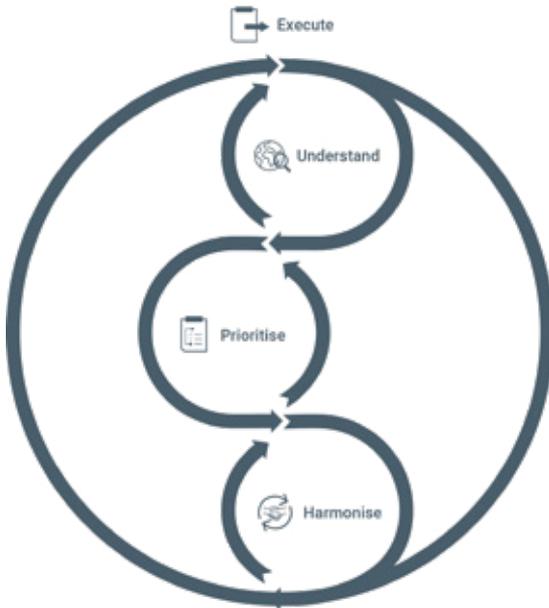
Figure 15 Process model of self-synchronisation

Understand is where nodes aim to achieve insight in the network and make sense of the mission environment. The understand loop comprises situational awareness and self-assessment. Situational awareness concerns gaining knowledge about the mission environment and about other nodes within the environment. Self-assessment focuses on the state of a node's own capabilities, at least to the extent nodes are capable of conducting activities. To be effective, self-synchronising nodes need at least a basic understanding of the environment, capabilities of other nodes and intentions of actors, as well as knowledge of foreseen challenges and possible mitigation measures. Situational awareness itself is not a 'stable state'; meaning it will develop iteratively, change continuously and become more thorough as a result of interactions between nodes and the mission environment (i.e. conducting activities and analysing the effect of these activities). Understanding enables the interaction and collaboration between nodes, for example through identifying nodes with similar understanding of challenges in the mission environment, connecting with them and gaining awareness of individual node intent, and through harmonising towards

a specific approach to tackle the challenge together. An effective self-synchronising node will develop some degree of shared situational awareness over time, by harmonising with other nodes that may have a different awareness of the situation.

Prioritise enables nodes to assess and agree the optimal (set of) activities to execute. Although all nodes will need to prioritise their own individual possible actions, prioritisation may be influenced and shaped by the needs and priorities of other nodes. Prioritising activities is conditional on the understanding of the mission environment. However, it is neither necessary nor possible to fully understand a situation in advance, conversely it is necessary to observe and learn from the effects after execution, and by doing so to increase the level of understanding and prioritisation.

Harmonise is the loop in which nodes exchange and align their observations, assessments, intentions, plans and actions with other nodes. It runs continuously with understand, prioritise and execute by building on the understand and prioritise loops which are then fed from the execute loop. The aim of harmonisation is to identify and agree with other nodes on (shared) goals and intents, overcome problems in the mission environment, generate solutions on how to solve these problems, and how to come to decisions.[18] If nodes agree to work closely together in a temporary sub-network, they need to agree on which other nodes to include within this sub-network. Outcomes such as 'agree to disagree', co-existence and deconfliction are also valuable forms of harmonisation.

Execute entails nodes conducting prioritised activities, delivering effects to impact the mission environment and to influence actors. Assessing whether these activities achieve desired objectives will inform the understand loop and drive the continuous nature of the overall self-synchronisation process. While executing, nodes continuously update their understand, prioritise and harmonise processes. Nodes may also test preliminary decisions and evaluate alternative decisions. This can either be done within a temporary sub-network or between harmonised nodes. Nodes working together in a temporary sub-network will organise temporary process control. The execute loop is where self-synchronised activities can best be observed.

For each loop, specific mechanisms are identified that enable self-synchronisation. We distinguish mechanisms that could drive self-synchronisation and mechanisms that could support the process of self-synchronisation. Some of these mechanisms provide supporting techniques for self-synchronisation, such as tools, checklists, or process steps. The combination of the loops of self-synchronisation and the corresponding mechanisms provides insight in the internal process of the loop and in how the loops can fluently merge into each other. There is not only one way to progress through this process of self-synchronisation, multiple options exist to self-synchronise.

---

18. Such as the manner in which decisions are made, including rules and criteria.

The **mechanisms that could drive the process of self-synchronisation** can be found in the table below.

	Loop	Mechanism	Description
	Understand	Mechanism to imply overarching (strategic) direction and guidance	Freedom to decide; a shift from order to mandate. A mandate provides direction via the unacceptable conditions to address, and constraints and restraints.
	Understand	Default information requirements	The required level of information about other nodes, for each phase of ad-hoc collaboration. Relevance depends on: a) overlapping spheres of influence and b) interdependencies between the nodes.
	Understand	Self-image	Image theory (Beach & Mitchell, 1990) provides a theoretical basis to define e.g. how different nodes value their situation, how they intent to influence the situation and what goals they want to achieve. Self-image concerns beliefs, morals, ethics, rules, values, norms, etc.

The table below provides examples of **mechanisms that could support the process of self-synchronisation**. For the full list of mechanisms including descriptons of the mechanisms we refer to the MCDC report.

	Loop	Mechanism	Description
	Understand	Mechanism to prioritise activities	Activity priority assessment: checklist to assess the best (set of) activities in relation to the context.
	Understand	Mechanism to align and coordinate activities	Extended Traffic Light System: compresses way of communicating the support opportunities of other nodes. The system consists of four states (green, yellow, orange and red).
	Prioritise	Mechanism to align and coordinate activities	Capability assessment: method to assess whether a node can perform intended activities by itself, or if cooperation is needed.

	Harmonise	Mechanism to align and coordinate activities	Capability gap assessment: based on the activity priority and the capability assessment, nodes address capability and capacity gaps. Support assessment: checklist to assess the possibility that another node is willing to provide capacity support or is open for cooperation. Legitimacy mechanism: Provides insight in perceived legitimacy which is based on perceptions and expectations.
	Harmonise	Mechanism to harmonise priorities, intentions and plans	The essence of this mechanism is to come to shared assessments and intentions that will allow the identification of roles and responsibilities and enable nodes to harmonise. Key elements are respect and understanding, the will to share information (transparency), impartiality and credibility, and engage and enable. Supporting techniques are: • Dialogue and Sharing • Respect and Understanding • Engage & Enable • Adaptive campaigning • Divide roles and responsibilities
	Harmonise	Mechanism to form, re-form, and de-form self-synchronising subnetworks	This mechanism includes a check-list to support nodes to keep a holistic view on the situation while maintaining focus on mutual interests, activities and goals.
	Harmonise	Mechanism to establish and update commonly agreed & understood rules of engagement that enable self-synchronisation	A checklist and method to document commonly agreed work agreements within a subnetwork.
	Execute	Mechanism to support planning during execution	Search of alternatives: are there alternative approaches to address the selected problem? Test and anchor decisions: decide upon an approach within the ad-hoc collaboration. Process control: work arrangements on how to collaborate to execute the selected approach.

Enablers of self-synchronisation

Self-synchronisation is enabled by trust, ability to adapt, a high level of knowledge of own and other actors' capabilities and the mission environment, and shared mental models (Cebrowski & Gartska, 1998). How these enablers will support self-synchronisation in the process described above, varies per enabler. Trust determines the extent to which nodes are willing to contribute and the nature of the interaction or collaboration that takes place (Alberts & Hayes, 2006). The question is, how to build trust as quickly as possible and then maintain and facilitate it, while for adaptability the issue is how nodes can select the appropriate structure to cope or shape unanticipated events. Trust is also needed for senior leaders within a parent organisation to give up personal control and totally rely on field level nodes for the execution of activities, which may be their subordinates in the formal (parent) organisation. Nodes must also trust each other and the products, capabilities and services which are provided to take the correct action within the framework of strategic guidance. Trust should help to interpret things similarly and trust should contribute to reacting the same way to a particular situation (Hutchins et al., 2001).

Flexibility and adaptability are often described as the main characteristics of a network operating in a self-synchronised manner. However, in order to do so, nodes should also possess the ability to adapt and to be able to cope with and expect a high level of uncertainty. This is described by Beautement (2006) as "the ability to adapt to (or shape) change; to be innovative, flexible and responsive (and grasp fleeting opportunities) and to be robust and resilient (in the face of potentially catastrophic disruption)". Adaptability could be realised by adopting multifunctional modularity in the composition of nodes (assuming that these 'modular' nodes could be changed fast enough during operations) or the ability to form sub-networks and reform quickly, depending on what is most relevant. Sub-networks can change their "operational system", i.e. the way that they structure and organise themselves, interact and process (Beautement, 2006). For example, a subset of nodes will come together to work on a particular problem and then go back to their original activities once the problem is taken care of (Hutchins et al., 2001).

Knowledge of own and other actors' capabilities will be strongly supported with the help of IT systems, yet this will put more emphasis on the importance of a standardised rule set of exchanging information. Shared mental models are required to achieve unity of effort and will develop over time, as nodes actively engage in the process of self-synchronisation and the harmonisation of priorities and activities.

Consequences for the principles of command and control

At the beginning of this section we asked the question whether the traditional principles of command and control (unity, continuity, integration and clarity) as described in section 1.5 will still stand when nodes operate in a self-synchronised manner? As also stated in section 1.5, NetForce should meet these principles, as they represent a core function of command and control that remains relevant, also when operating in a self-synchronised way. However, the traditional implementation of the principles does not seem to fit with self-synchronisation, as the traditional implementation is based upon an organisation with a (single) hierarchical chain of command and with prescriptive processes for the entire organisation. Therefore, we argue that although the principles remain relevant, the implementation of these principles needs to change for NetForce Command.

The current implementation of the principle unity is based on shared objectives and goals by means of coherent preparation and planning between all included elements. Successful self-synchronisation is based on planning that emerges ad-hoc and locally within the nodes and between the nodes (Bemmel et al., 2017). This means that while integrated planning for activities in a self-synchronising network will be difficult, the preparations and planning of actions can still be executed within temporary sub-networks. With regard to creating unity of effort, rather than joint planning, coordination and cooperation between all elements, the focus in self-synchronisation will be more on harmonising priorities, intentions, and plans.

Although the principles remain relevant, the implementation of these principles needs to change for NetForce Command.

If we take the principle of continuity it is safe to say that the traditional implementation is based on advanced planning for the direction, coordination and organisation (e.g. control) of armed forces. Self-synchronising nodes also require harmonised goals and activities throughout an operation to achieve common objectives. With regard to the performance of activities conducted by a node, temporary sub-network, this will be a continuous activity. In this case the identified goals and activities will disappear as well to be replaced by new ones, falling out of continuous feedback loops and planning and harmonisation. This approach implies that there is no mission design, at least not initially. Objectives, lines of operation and missions are not specified but implied by overarching (political) guidance, the mandate (objective and purpose) and fields of expertise of the nodes in the network. In the context of self-synchronisation, a dynamic mission design may emerge at field level. This approach does not mean that there is no planning at all. It means working towards the horizon in the perceived operational reality instead of over the horizon as in the current hierarchical approach. In the case of maximum self-synchronisation, however, support and maintaining purpose and harmonisation of efforts and effects over time is more of a challenge. How to guarantee continuity throughout the entire self-synchronising network, is subject for further research.

Clarity also continues to be a relevant principle when dealing with self-synchronisation. Although in this case, it does not pertain to a clear chain of command, but to a clear understanding of intent. The overall goal, purpose, intent, and/or mission must be known by every node and every node must direct their efforts toward achieving it (Araki, 1999). Of course sub-goals (e.g. personal goals of the different nodes within the network) will remain and may differ between nodes, but this does not mean that these sub-goals do not correspond to the overall objective. In self-synchronising networks this structure is not hierarchical but based on expertise and skills.

Finally, the principle of integration. Nodes can become part of NetForce when their capabilities are useful and contributory and they can leave the network any time. A self-synchronising network is therefore not a formal organisation with clear tasks, roles and functions and nodes will often pursue different objectives related to the organisations they represent. Integration of capabilities and activities is a challenge because you cannot simply arrange, command or control it. It has to follow from different forms of motivation. Self-synchronisation will focus more on organising and harmonising visions and efforts between nodes, rather than on integrating capabilities and activities.

Concluding remarks

Self-synchronisation means that the function of command and control and related decision authority is implemented at field level, where empowered nodes operate and synchronise activities with other nodes in NetForce. The process of self-synchronisation can be described by the loops understand, prioritise, harmonise and execute, including their associated driving and supporting mechanisms. These processes and mechanisms enable self-synchronisation in the overall NetForce Command concept. In chapter 4 you can read what self-synchronisation can look like and how other concepts like decision making, collaboration and information management are linked with the self-synchronisation concept. Implementation of self-synchronisation has implications for military nodes and the armed forces in general. In chapter 6 we provide a broad overview and analysis of the implications along the DOTMLPFI[19] lines, which are essential factors for developing and implementing the capability NetForce Command. More information on self-synchronisation can be found in the further reading suggestions below.

Further reading

Kuijt, J.T., van de, Eikelboom, A.R., Benda, R., Pieneman, R. (2017) V1604 Self-synchronisation and orchestration as alternative approaches to traditional C2. TNO report: TNO 2017 R11573, Den Haag: TNO.

Eikelboom, A.R., Kuijt, J.T. van de, Benda, R., Pieneman, R. & Bemmel, I.E. van (2018). Self-synchronization as additional approach to traditional C2. Paper presented at 23rd International Command and Control Research & Technology Symposium (ICCRTS) 2018, 6-9 November, Pensacola, Florida (USA). http://internationalc2institute.org/proceedings.

---

19. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

3.2   Orchestration

In chapter 2 we introduced NetForce Command as a networked approach of command and control in which collaboration and information sharing between capabilities are paramount and the function of command is shared with or distributed between civilian and/or military capabilities contributing to a NetForce. There are different implementations of a networked approach of command and control, in other words different implementations of NetForce Command. The most extreme implementation of NetForce Command can be characterised as self-synchronisation (see section 2.1).

But what type of command is needed to help nodes harmonise their activities if self-synchronisation does not arise, is not desired and does not seem to work? In those cases different manifestations of orchestration may arise to support harmonisation, to increase operational tempo and adaptivity and to create unity of effort of the military and civilian capabilities in the NetForce. The less extreme implementation of NetForce Command is therefore the one that can be characterised as maximum orchestration.

What is orchestration?

But what is orchestration? According to the Australian Ministry of Defence orchestration concerns the 'arrangements of physical and non-physical actions to ensure their unified contribution to the mission' (Australia Ministry of Defence, 2009). In Ascalon (Land Warfare Centre, 2017) orchestration is defined as the organisation of tactical tasks and activities within one or between multiple operations in order to achieve effects in the three environments (human, physical and information environment).[20] The Royal Netherlands Army (RNLA) defines orchestration as the planning, preparation and conducting of tactical military activities, including giving clear direction, aimed at achieving effects (Land Warfare Centre, 2014). Orchestration concerns bringing together, combining, integrating and organising different capabilities of an operation. In other words, the synchronisation of different capabilities and processes within activity or between multiple activities.

> " Orchestration concerns bringing together, combining, integrating and organising different capabilities of an operation."

We define orchestration as **an extreme form of harmonisation support**, provided by orchestrating elements. Harmonisation support is focused on creating unity of effort in a mission environment and is provided to the nodes and temporary sub-networks in NetForce. Harmonisation support is provided and received based on mutual consent, which means there is no hierarchical relationship between the elements that provide harmonisation support and the nodes and temporary sub-networks that receive harmonisation support. Because these relationships are functional and often informal, the civilian and military capabilities can decide not to accept and not to use the

---

20. Conflict is not restricted to the physical environment, but also takes place in the human environment (e.g. attitudes, mindset, social connections) and the information environment (e.g. (social) media, digital platforms). Interventions directed against these environments need to be coordinated simultaneously.

harmonisation support.[21] When maximum orchestration has the character of guidelines and orders, the approach to command and control is hierarchical. In that case we no longer speak of NetForce Command, but of orchestration in an hierarchical implementation of command and control.

Orchestration in the form of harmonisation support provided by orchestrating elements is challenging, because why should nodes accept harmonisation support when they have a right to disregard the support and do not have a hierarchical relationship with the orchestrating element? And what is an orchestrating element? How is an orchestrating element formed? How does an orchestrating element function? And how does it maintain its value for the nodes and temporary sub-networks in NetForce?

What is an orchestrating element?

An orchestrating element supports harmonisation of nodes and temporary sub-networks in NetForce by creating shared situational awareness and by providing harmonisation support for designing, planning, and attuning and aligning of activities in order to realise desired effects in the mission environment. In other words, orchestrating elements may provide synchronisation of the processes and activities of nodes and temporary sub-networks in NetForce by taking on the following functions:

By supporting shared situational understanding that is conditional for harmonisation (shared situational understanding);[22]

By supporting the harmonisation process of developing a dynamic tactical design and translating that design into harmonised activities (designing);

By supporting the harmonisation process of determining how to use military and civilian nodes (the means) and by whom in time and space to realise objective(s) (planning); and

By supporting the harmonisation process of coordinating the execution of activities by military and civilian nodes to realise objective(s) (attuning and aligning).

21. However, there are circumstances in which military capabilities need (extreme) harmonisation support to align military activities and cannot afford to disregard the harmonisation support, for example to prevent risks like friendly fires incidents.
22. An orchestrating element supports creating shared situational understanding. The sensing process needed to develop situational understanding is not a function of an orchestrating element. Within the TNO research programme Sensing in a networked environment (SiaNE) sensing nodes and sensing management elements are responsible for the sensing process.

Function and purpose of orchestrating elements
Orchestrating elements are command elements in NetForce that support harmonisation of the activities of collaborating military and non-military nodes in NetForce by contributing to shared understanding and by providing harmonisation support for designing, planning, and attuning and aligning activities in order to realise desired effects in three environments (human, physical and information).

How is an orchestrating element formed?

The need for some level of orchestration is determined by the gap between the requirements of the mission environment and the abilities of the nodes and temporary sub-networks in NetForce. Based on the need for some level of orchestration orchestrating elements are formed. They are either formed bottom-up by the nodes and temporary nodes or top-down by a strategic coalition and/or the parent organisations.

Orchestrating element formed bottum-up
A desire for more coordination and harmonisation is often the reason for orchestrating elements to emerge in a self-synchronising NetForce.
When a desire for coordination and harmonisation occurs bottom-up a self-synchronising NetForce is slowly transformed into a more coordinated NetForce where orchestrating elements may provide harmonisation support. An orchestrating element may be formed by two or more nodes, but it can also be formed out of an already existing temporary sub-network.

Orchestrating element formed top-down
A strategic coalition or one or more parent organisations may also decide to form an orchestrating element to harmonise activities. Besides harmonisation, a strategic coalition or the parent organisations may have other, often more political reasons (more political influence and power, trade interests and agreements, etc) to form an orchestrating element. Orchestrating elements that are formed top-down are probably composed and organised faster than orchestrating elements that are formed bottom-up.

After the formation in the positioning phase in the four phases of interaction and collaboration (as explained in section 2.3), the forming of an orchestrating element is started during the shaping phase of interaction and collaboration.

What are the characteristics of an orchestrating element?

There are numerous manifestations of orchestrating elements. The manifestation of an orchestrating element and the harmonisation support it provides, depends on the group dynamics process of social interaction in the shaping phase, which influences the following characteristics of an orchestrating element: function and purpose, the composition, organisation and structure, culture, and style of orchestration.

- **Composition:** the composition of an orchestrating element is determined by the type and diversity of nodes that contribute to an orchestrating element, the amount of nodes, and the density of participating nodes and their familiarity with each other (e.g. connectedness). The composition of an orchestrating element influences the behaviours of the nodes represented in an orchestrating element;
- **Organisation & Structure:** the organisation and structure of an orchestrating element is dependent on the objective and organisational aspects like role division (tasks, responsibilities and authorities), work processes and agreements, leadership, decision-making, control, communication and information exchanges. The organisation and structure of an orchestrating element influences the behaviours of the nodes represented in an orchestrating element;
- **Culture:** the culture of an orchestrating element pertains to the underlying beliefs, assumptions, values, norms, systems (formal/informal), symbols, language, habits and ways of communication of an orchestrating element. Culture influences the behaviours of the nodes represented in an orchestrating element and how people interact, collaborate and share information;
- **Style of orchestration:** the style of orchestration refers to the way an orchestrating element performs its function in its interactions with the nodes and temporary sub-networks. The style of orchestration is influenced by the bottom-up or top-down formation of an orchestrating element and on the extent harmonisation is needed. Examples of orchestration styles may vary from supporting, facilitating, coordinating, and coaching to managing, directing and controlling.

When an orchestrating element is formed, it can provide harmonisation support to nodes and temporary sub-networks in NetForce. In the executing phase the functioning of an orchestrating element becomes apparent and will be changed or transformed based on developments in the mission environment. The forming of collaboration in an orchestrating element is depicted in Figure 16.
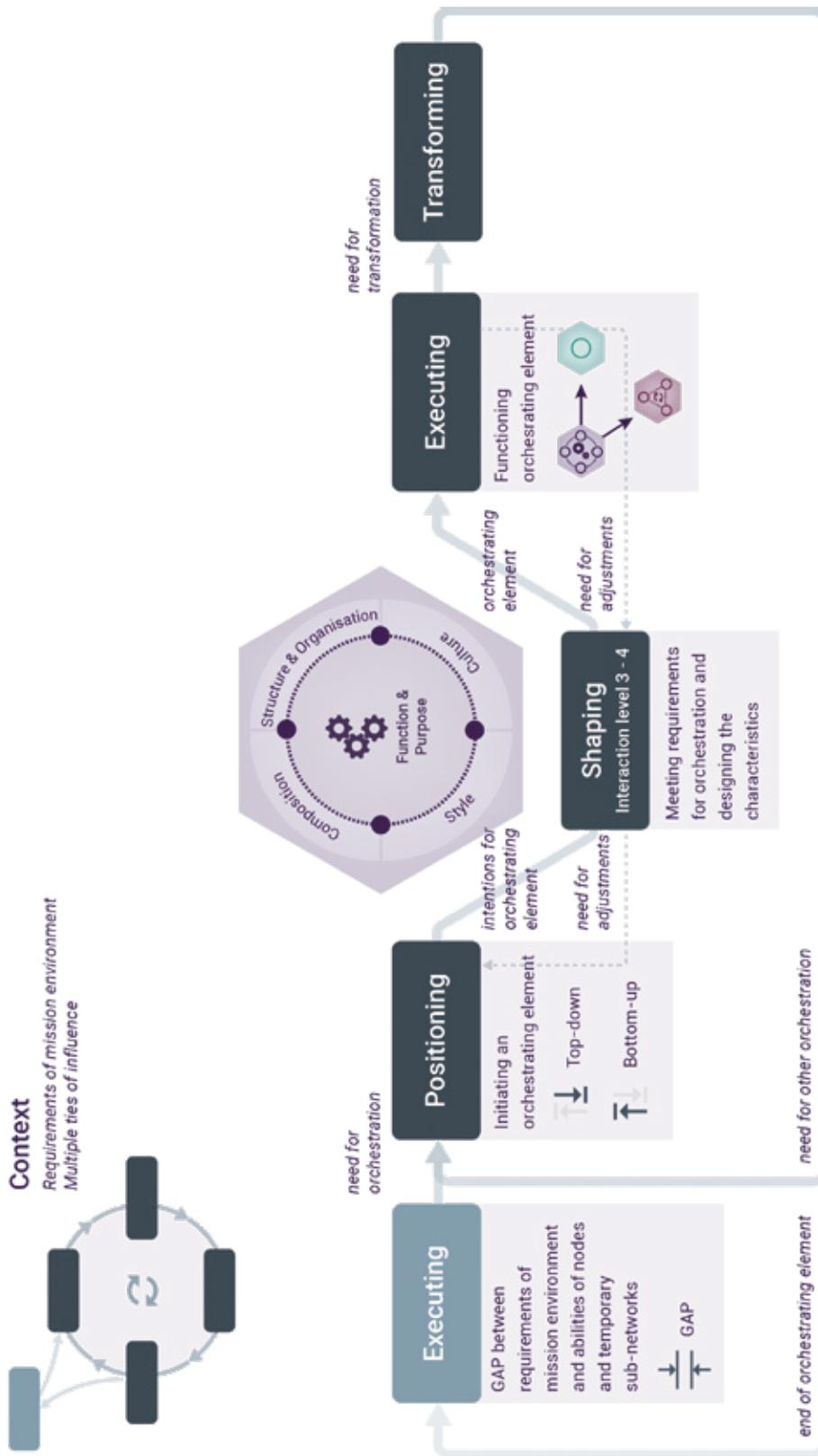
Figure 16 Process model for forming of collaboration in an orchestrating element

Manifestations of orchestrating elements

Having explained the characteristics of orchestrating elements, it is still unclear how the infinite manifestations of orchestrating elements may differ from each other. To be able to identify different manifestations of orchestrating elements we need to understand which variables influence the purpose and function of the orchestrating element, the composition, the organisation & structure, the culture and the style of orchestration towards the nodes and temporary sub-networks in NetForce. We identified a set of ten key variables that determine the characteristics of a manifestation of an orchestrating element. These ten key variables are included in a support tool that can be used for describing a manifestation of an orchestrating element. The support tool depicts five steps for describing the manifestation of an orchestrating element.

Step 1: function and purpose variables

The first step includes the variables to describe the function and purpose of the orchestrating element. It includes the variable to describe the function of the orchestrating element. Contributing to shared situational understanding, and providing harmonisation support for designing, planning, attuning and aligning of activities are the four function options of orchestrating elements. The four functions for orchestrating elements are interrelated, but it is possible that an orchestrating element fulfils one or more functions and not all four. It may for example support developing a dynamic tactical design, but not support the planning of different activities. The amount of functions that an orchestrating element fulfils, determines the type and the diversity of nodes that are needed in the orchestrating element. And lastly, the intended level of harmonisation support that is needed (on a continuum from low to high) to support the nodes in the NetForce will also determine the manifestation of an orchestrating element. Depending on what is needed for the nodes in NetForce (support for creating shared situational awareness, designing, planning or attuning and aligning activities) a different level of harmonisation support is required.

Function and Purpose		
Function (More than one applicable)	Shared situational understanding	Design
	Planning	Execution
Intended level of orchestration (external interaction)	Low	High

Step 2: composition variables

Step 2 includes the key variables that describe the composition of orchestrating elements. The composition is determined by the amount of nodes (size) that contribute to the orchestrating element. The size of the orchestrating element will influence its organisation, structure and culture, and is therefore an important variable to include in the support tool. For example, it is expected that the structure of an orchestrating element will be flat when there are a limited number of participants who are responsible for many activities. When the orchestrating element includes many participants, it may require a more complex structure. The diversity of the nodes and sub-networks that an orchestrating

element supports also influences the composition of an orchestrating element. The composition of an orchestrating element will differ depending on whether it supports a heterogeneous or homogeneous set of nodes and related temporary sub-networks.
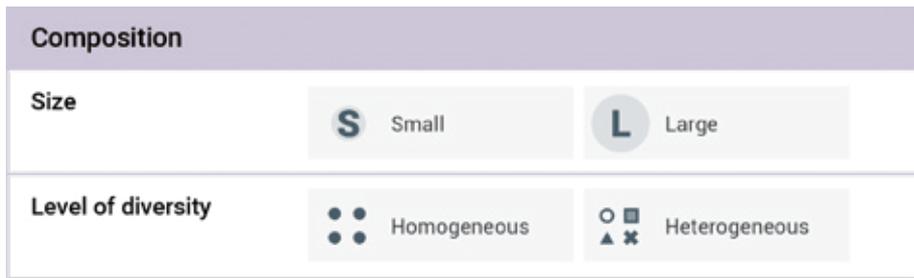
Step 3: organisation & structure variables

Step 3 includes variables that describe the organisation and structure of the orchestrating element. The first variable relates to the command and control organisation of the orchestrating element. For example, a single person could be responsible for making important decisions and performing a leadership function. However, if the environment is too complex, dynamic and insecure for one single leader to operate effectively, then leadership roles may be collectively shared among the members of an orchestrating element (see section 3.3) and decision-making will be preceded by negotiations (see section 3.4). Structural aspects of the orchestrating element (from networked to hierarchy) influence the collaboration and way of working between the members of an orchestrating element. It also influences the role division (tasks, responsibilities and authorities), work processes and agreements and communication and information exchange.
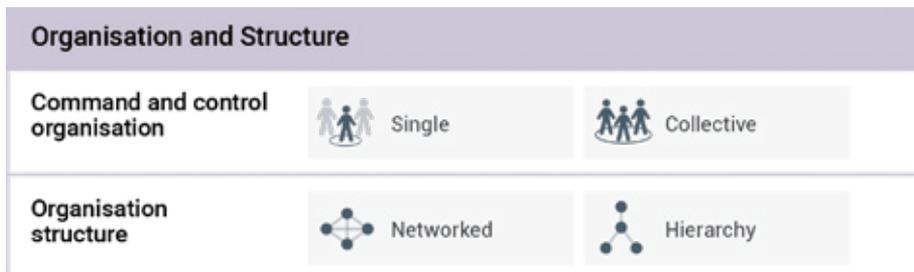
Step 4: culture variables

Step 4 includes variables that describe the culture of an orchestrating element. The members of the orchestrating element develop the culture of an orchestrating element, for example how formal or informal the orchestrating element is organised and which underlying beliefs, assumptions, norms, and values are acknowledged as important. The culture of an orchestrating element also reflects to what extent the orchestrating element is open to external new and innovative ideas and solutions (orientation) and to what extent an orchestrating element is able to adapt its harmonisation support, its work processes and solutions to changes in the mission environment and the need of the other nodes in NetForce (adaptability).

Culture		
Degree of formalisation	Formal	Informal
Orientation	Internal	External
Adaptibility	Robust	Agile

Step 5: orchestration variables

Step 5 includes the variable that describe the style of orchestration towards the other nodes in the NetForce. The style of orchestration describes the way an orchestrating element provides harmonisation support to the nodes and temporary sub-networks. It describes the types and styles of leadership, the use of power in decision-making, and the degree of seeking control. It is expected that an orchestrating element will tailor its orchestration style depending on the problem context and the extent of harmonisation that is needed to support the nodes. An orchestrating element is more supportive if it is focused on empowering and engaging the nodes and temporary sub-networks in NetForce. When an orchestrating element imposes control over the other nodes in the NetForce, it is expected to have more influence, dominance and power.

Taken together the ten key variables for to the purpose and function of an orchestrating element, the composition, organisation and structure, culture, and style of orchestration lead to the support tool as shown in Figure 17. The support tool consists of the aforementioned 5 steps and serves as a guideline for describing the manifestation of an orchestrating element in more detail but can also be used for formation and implementation of an orchestrating element.

Style (external behaviour)		
Style of orchestration	Supporting	Control

Function and Purpose				
Function	Shared situational understanding	Design	Planning	Execution
Intended level of orchestration (external interaction	Low ├──────────────┤ High			

Composition	
Size	Small S ├──────────────┤ L Large
Level of diversity	Homogeneous ├──────────────┤ Heterogeneous

Organisation and Structure	
Organisation structure	Networked ├──────────────┤ Hierarchy
C2 Organisation	Single ├──────────────┤ Collective

Culture	
Degree of formalisation	Formal ├──────────────┤ Informal
Orientation	Internal ├──────────────┤ External
Adaptibility	Robust ├──────────────┤ Agile

Style (external behaviour)	
Style of orchestration	Supporting ├──────────────┤ Control

Figure 17 Overview of key variables

Towards archetypical orchestrating elements

Based on the support tool, there are 1024 (2^{10}) possible manifestations of orchestrating elements. Because this means there are still many manifestations, we tried to distinguish a few archetypical orchestrating elements based on the key variables. Archetypical orchestrating elements are relevant to distinguish for different purposes:

• Experimentation with orchestrating elements;
• Discussing the functioning of orchestrating elements;
• Education and training for working in/with orchestrating elements;
• Further developing the concept of orchestrating elements;
• Describing orchestrating elements in doctrine publications.

We expect that the function and purpose of the orchestrating element determine the manifestation of an orchestrating element the most. When the function and purpose change, the composition, organisation and structure, culture and style of orchestration of an orchestrating element will automatically alter as well. Therefore, we concluded that the variables under function and purpose: 1) the function(s) to support and 2) the intended level of harmonisation support are the key variables that can be used to distinguish the archetypical orchestrating elements. When considering these variables as the key variables, we can distinguish four different archetypical orchestrating elements. Below these four different archetypical orchestrating elements are listed and visualised (Figure 18):

• Orchestrating element provides support for one function and provides a low level of harmonisation support;
• Orchestrating element provides support for two or more functions and provides a low level of harmonisation support;
• Orchestrating element provides support for one function and provides a high level of harmonisation support;
• Orchestrating element provides support for two or more functions and provides a high level of harmonisation support.
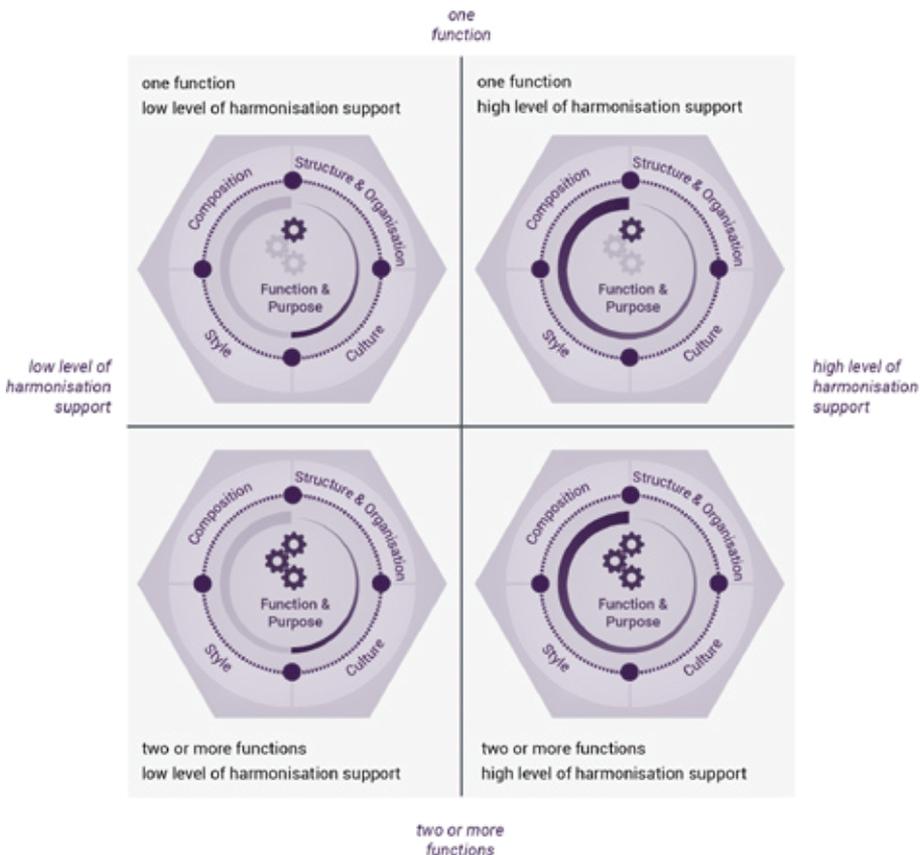
Figure 18 Four different archetypical orchestrating elements

Concluding remarks

In NetForce orchestration is an extreme form of harmonisation support, focused on creating unity of effort between nodes and temporary sub-networks. Harmonisation support is provided by orchestrating elements. They can contribute to the creation of shared situational awareness and they can harmonise designing, planning, attuning and aligning of activities. In chapter 4 an orchestrating element becomes more tangible in archetype B and C. You can read how an orchestrating element is formed and how it may function in archetype B and C. Orchestration in the form of harmonisation support by orchestrating elements have implications for military nodes and the armed forces in general. In chapter 6 we provide a broad overview and analysis of the implications along the DOTMLPFI[23] lines, which are essential factors for developing and implementing the capability NetForce Command. More information on orchestrating elements can be found in the further reading suggestion below.

Further reading

Kuijt, J. van de, Bemmel, I.E. van, Benda, R, & Roelofs, M. (2019). V1604 Functioning of orchestrating elements in NetForce: a blueprint. TNO report TNO 2018 R11450. Den Haag: TNO.

---

23. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

Watch the explanimation Leadership in NetForce.

3.3   Leadership in NetForce

Complex, dynamic and networked mission environments require agile approaches focused on exploration, experimentation, creativity and learning that make it possible to adapt and do the right things in the environment. However, most organisations that contribute to NetForce with one or more nodes are hierarchically structured and organised to do things in a cost-effective and right way. They apply robust approaches focused on exploitation, alignment, correction and control to cope with the environment. This creates tension between what the context requires and what most organisations are capable of doing ('t Hart et al., 2016; Duijnhoven et al., 2017).

Many organisations respond by increasing and improving their robust approach, which will often increase instead of solve the tension. Too much robustness will even lead to rigidity and bureaucracy. However, 100% agility of organisations will lead to chaos. To cope with this tension a robust as well as agile approach is needed ('t Hart et al., 2016; Duijnhoven et al., 2017): doing the right things in the right way.

Coping with the complex, dynamic and networked environment by applying a robust as well as agile approach is called ambidexterity. Ambidexterity is defined as the capacity of an organisation to be "aligned and efficient in their management of today's business demands while simultaneously adaptive to changes in the environment" (Raisch & Birkinshaw, 2008, p. 375). To be effective in a constantly changing and unpredictable environment, an organisation has to be able to balance between improving alignment to current environments and increasing efficiency on the one hand, and increasing variety and adaptability on the other hand. In other words, to maintain long-term adaptability and viability, the tension between the need to innovate (often external pressures) and the need to produce (mostly internal pressures) needs to be balanced (Uhl-Bien & Arena, 2018). A robust as well as agile approach as depicted below can create that balance.
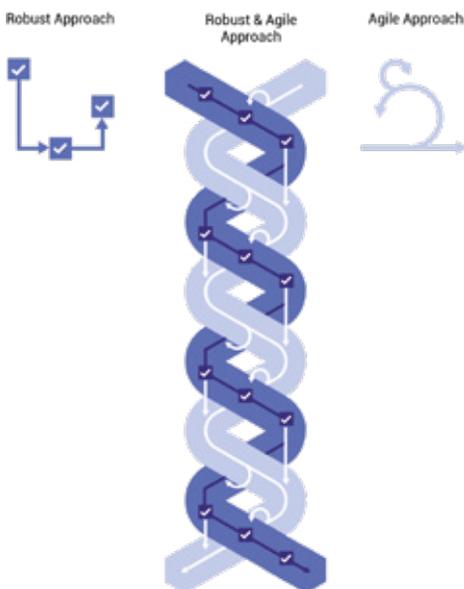

Figure 19 Overview of approaches

The challenge for leadership in NetForce is to deal effectively with this tension and to influence the balance between robustness and agility. This challenges leads to the following question: What type of leadership is needed to cope with this challenge? More specifically, what type(s) of leadership may be effective within nodes and parent organisations? For the NetForce collaborations the challenge is even bigger, because who is in the lead in temporary sub-networks, orchestrating elements and strategic coalitions, where in theory all contributing actors are equal? And what type(s) of leadership are effective in these collaborations?

Ambidextrous leadership in NetForce

Leadership in the armed forces is already studied and described in much detail and leadership theory for the armed forces is well developed (Dalenberg et al., 2014). However, in light of current trends and developments as described in chapter 1, a new scientific research approach to leadership seems to emerge with relevancy for leadership in NetForce, which will often be in complex, dynamic and networked mission environments. This new scientific approach seems to focus on coping with complexity and includes new theories on leadership, for example emergent leadership, collective leadership, shared leadership, distributed leadership, distanced leadership, complexity leadership and ambidextrous leadership. We explored whether these theories could support the development of a concept for leadership in NetForce as an addition to existing theory on leadership in the armed forces.

Based on our literature review and analysis (Van Bemmel & Van der Boor, 2019), ambidextrous leadership (Rosing et al., 2011) is the type of leadership that seems to fit best as the basic leadership approach for nodes, parent organisations and collaborations in NetForce. Ambidextrous leadership makes it possible to constantly adjust the balance of robust and agile approaches in order to deal with the tension between what the context requires and what most organisations and collaborations in NetForce are capable of doing.

Ambidextrous leadership is the type of leadership that seems to fit best as the basic leadership approach for nodes, parent organisations and collaborations in NetForce.

Ambidextrous leadership consists of three elements (Rosing et al., 2011):

1. closing leader behaviours to foster exploitation (robust approach),
2. opening leader behaviours to foster exploration (agile approach),
3. and the temporal flexibility to switch between both as the situation requires. Being able to switch between these types of behaviours and thereby creating an effective balance is necessary to maintain effectiveness in a continually changing environment.

The theory of ambidextrous leadership can be enriched with the three forms of leadership in the complexity leadership framework (Uhl-Bien & Arena, 2018, p. 98):

Closing leader behaviours are similar to operational leadership and foster exploitation (the robust approach). **Operational leadership** is defined as "leadership in the formal systems, structures and processes that produces results through selection, refinement and efficiency". Operational leadership has a strong focus on stability, planning, coordination, alignment, and control.
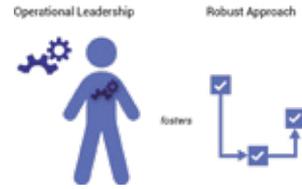

Opening leader behaviours are similar to entrepreneurial leadership and foster exploration (the agile approach). **Entrepreneurial leadership** is defined as "leadership that works to create new knowledge, skills, products and processes" to sustain the future viability of an organisation. Entrepreneurial leadership has a strong focus on flexibility, organic and emergent processes that promote experimenting and learning.
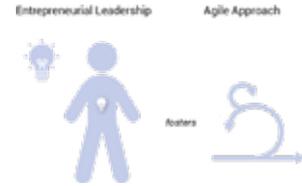
The ability to switch and conduct the balancing act for a robust as well as agile approach is facilitated by enabling leadership. **Enabling leadership** sets the conditions for switching and conducting the balancing act for a both robust and agile approach. **Enabling leadership is focused on creating, engaging and protecting the "adaptive space" needed to nurture and sustain the adaptability process in organisations.** This type of leadership enables adaptive space and the adaptive process that supports and catalyses entrepreneurial leadership and that connects the results of entrepreneurial leadership to the formal systems, structures and processes governed by operational leadership. One could argue that enabling leadership creates a bridge between operational and entrepreneurial leadership and therefore enables ambidextrous leadership, which is focused on applying a balanced both robust and agile approach for the situation at hand. Enabling leadership does so "by creating structures and processes (e.g. semi structures, temporary decentralisation, collaboration, brokering, network cohesion, adaptive capabilities, absorptive capacity) that effectively engage conflicting (i.e., tension) and connecting (i.e., integration) to trigger and amplify emergence (i.e., innovation, adaptive responses) into new adaptive order (i.e., reintegration) for the organisation (i.e., transformation process).".
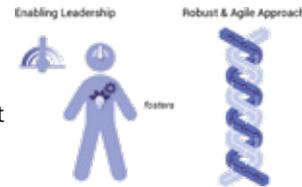
Most leaders are inclined to favour either operational leadership or entrepreneurial leadership. Ambidextrous leaders are capable of applying enabling leadership, which enables them to switch between and balance both operational and entrepreneurial leadership, despite their natural tendency to favour either operational or entrepreneurial leadership in all contexts. The theory of ambidextrous leadership enriched with the content of the three forms of leadership of the complexity leadership framework is visualised below.
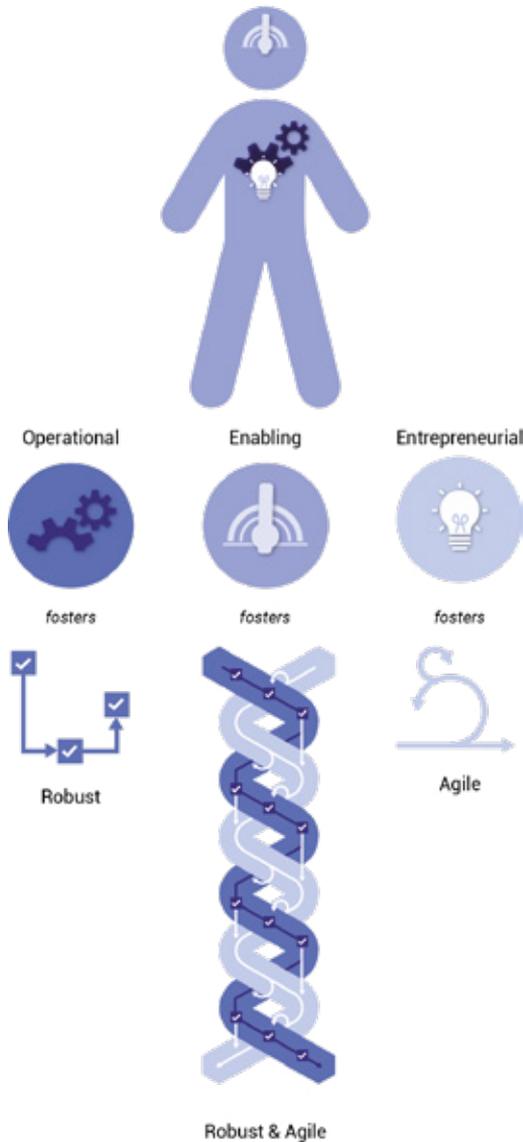
Figure 20 Ambidextrous leadership enriched with the complexity leadership framework

Ambidextrous leadership enriched with the three forms of leadership from the complexity leadership framework can be applied to leadership of parent organisations and nodes in NetForce. However, ambidextrous leadership is probably even more important for leadership that emerges in the group dynamic process of social interaction of NetForce collaborations in temporary sub-networks (archetype A, B and C), orchestrating elements (archetype B and C) and a strategic coalition (archetype C). The context of these NetForce collaborations is complex and dynamic, and therefore requires an agile approach. However, the participants (representatives of different nodes/parent organisations) in these collaborations have to deal with the influence of their parent organisations

(so called authority ties). Most parent organisations will be focused on realising their objectives in an efficient manner and apply a robust approach, which will not always be in line with the agile approach that is needed in the context and that is often favoured by the participants in the NetForce collaborations. The participants in NetForce collaborations have to reckon with the influence of the robust approaches of their parent organisations (doing things in the right way) and they need to balance these different robust approaches with the agile approaches that are needed in the complex, dynamic environment (doing the right things). Ambidextrous leadership is focused on precisely that; on dealing effectively with tensions between robust and agile approaches and holding a good balance to operate effectively in complex, dynamic environments. Therefore, ambidextrous leadership is necessary for leaders that emerge in NetForce collaborations. **To be able to perform ambidextrous leadership and to offer leadership in a broad range of contexts, the quality of enabling leadership is essential alongside a natural tendency for either operational or entrepreneurial leadership.**

Who is in the lead?

Leadership can manifest in different ways. Traditionally, leadership is performed by a single person, but in complex, dynamic and networked environments a commander/manager may not know and oversee everything. Furthermore, in collaborations of different actors, a leader is often not appointed, but emerges from the group dynamics within the group. In collaborations in which in theory all actors are equal, it may not even be desirable to have one leader. Therefore, we explored **collective leadership**.

When leadership is collective, the leadership influence is held by different people at different times and for different purposes. Collective leadership is often based on specific expertise, knowledge and skills and not so much on status or position. A wide variety of leadership theories are linked to collective leadership: shared leadership (Pearce & Conger, 2003), emergent leadership (Hogan, Curphy, & Hogan, 1994), distributed leadership (Brown & Gioia, 2002) and distanced leadership (Fair, Connaughton and Daly, 2004). These different forms of leadership have strong similarities and share characteristics of collective leadership:

- Leadership is not the monopoly or responsibility of just one person. The functions of leadership are **distributed** between different people or **shared** with more people.
- Leadership is a group activity, a **social process** that works through and within relationships, rather than individual action, which means that leadership **emerges** depending on the situation and context.
- Leadership will often be performed from a **distance**, from different parts in the network.

Based on the above we define collective leadership as a social process in which leadership emerges from the interaction of multiple actors of different organisations, the functions of leadership are distributed between different actors or shared with more actors, and leadership can be performed from a distance, from different parts in the network. Different forms of leadership are depicted in figure 21
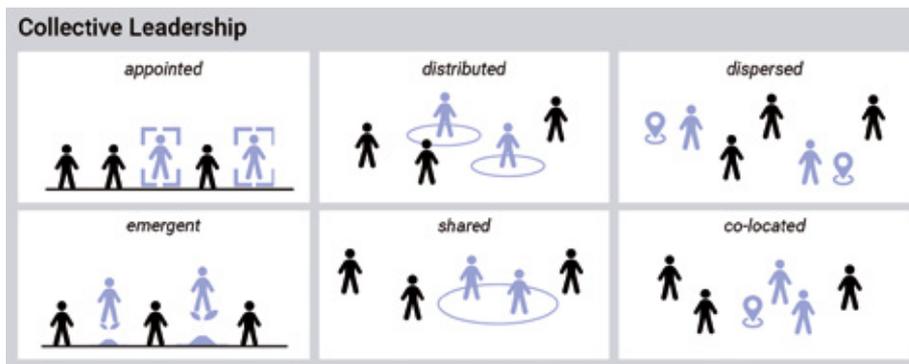
Figure 21 Collective leadership

In viewing leadership as a social process the perspective of the followers is important as well. Followership theory looks at both leaders and followers as co-producers of leadership and its outcomes (Uhl-Bien et al, 2014). According to this theory leadership is the result of a social interaction process between leaders and followers (as is collective leadership) and not the result of one's hierarchical position. An important assumption is that leadership cannot exist when there is no following behaviour. Furthermore, the theory acknowledges that leaders can also be(come) followers and that followers can be(come) leaders, as seems the case in NetForce. Following behaviours may manifest themselves in different forms (DeRue & Ashford, 2010):

• Granting power and influence to another person. Examples are succumbing, deferring, obeying or complying behaviour.
• Co-producing with another person. Examples are advising, challenging, correcting or persuading in a respectful and trusting way to generate more effective outcomes.

Following behaviours in combination with leading behaviours influence the form of collective leadership that will emerge, in other words how leadership will be shared and distributed and to what extent they will be performed from a distance.

Collective leadership seems very applicable to networked collaboration in NetForce, because collective leadership is defined as a social process in which leadership emerges from the interaction of multiple actors of different organisations and leadership is *distributed* between different actors or *shared* with more actors in NetForce, for example in temporary sub-networks and orchestrating elements. In these NetForce collaborations leadership emerges in the group dynamics of ad hoc collaboration and is likely to change over time to fit with the demands of the context. This implies that participants sometimes lead, and accept to follow at other times. Following behaviours in combination with leading behaviours influence the form of collective leadership that will emerge in NetForce. Although rare in practice, single leadership will also be possible in temporary sub-networks, orchestrating elements and strategic coalitions when the participants agree and chose to do so.

Although collective leadership and followership seem very applicable to NetForce collaborations, it seems less applicable to the often formal, hierarchical relationship within a parent organisation and the node(s) of that parent organisation in NetForce. However, when we make a distinction between leadership, decision-making and control (the three sub-functions of command in the armed forces of the Netherlands), collective

leadership is also possible in parent organisations and nodes that are hierarchically organised. Collective leadership and functional decision-making based on expertise, knowledge and skills are possible alongside overall decision-making authority and control by single formal managers or commanders, provided that these managers or commanders are open to the ideas and insights of their employees.

Manifestation of leadership in NetForce

In NetForce we envision ambidextrous leadership, enriched with the three forms of leadership in the complexity leadership framework (operational, entrepreneurial, and enabling leadership), and different forms of single and collective leadership to fit best as the principal leadership approach for military and civilian nodes, parent organisations and NetForce collaborations like temporary sub-networks, orchestrating elements and strategic coalitions.

Military and civilian nodes will of often need to apply ambidextrous leadership, more specifically enabling leadership and an emphasis on entrepreneurial leadership over operational leadership, to cope with the complex, dynamic and networked environment to which they contribute in NetForce. However, there are contexts in which the emphasis needs to be on operational leadership over entrepreneurial leadership. Enabling leadership is needed to make sure that the emphasis is in line with the requirements of the context and ambidextrous leadership is effective. Ambidextrous leadership in nodes will mainly manifest as single leadership, because many organisations are hierarchically structured and organised and a commander or manager is formally appointed. However collective manifestations are possible, especially when the nodes are informally organised and structured as a network. Furthermore, collective leadership and functional decision-making based on expertise, knowledge and skills may emerge alongside overall decision-making authority and control by single, formal managers or commanders.

Single, appointed ambidextrous leadership
often with emphasis on entrepreneurial leadership

Emergent , collective ambidextrous leadership in an armoured infantry platoon

The platoon commander is the formally appointed leader of an armoured infantry platoon. He will perform operational leadership influenced by the robust approach of his parent organisation, the armed forces. An emphasis on operational leadership is important in the process of becoming fully operationally capable. However, during deployment the environment becomes more complex and dynamic and an agile approach increases in importance. The platoon commander may change his leadership during deployment and will start to emphasize entrepreneurial leadership. When he has a natural tendency for entrepreneurial leadership (fostering an agile approach), this will be fairly easy for him. When he has a natural tendency for operational leadership (fostering a robust approach), he will experience tensions between the agile approach that is required in the environment and his tendency. For his platoon to be effective in a complex, dynamic mission environment, he needs to adopt a balanced both robust and agile approach and master ambidextrous leadership. To be able to adopt a balanced approach, a platoon commander needs to be open to the proposed agile and robust approaches of the (wo)men in his platoon. For example, a commander of an armoured infantry fighting vehicle (IFV) may come up with an idea for the creative deployment of the IFV (agile approach) and a communication specialist may provide an assessment of the associated communication risks (robust approach).

A platoon commander needs to take both (and other approaches) into account and develop a balanced both robust and agile approach. A platoon commander does not need to do this alone. A second in command should also master ambidextrous leadership to support a platoon commander and be able to develop a balanced approach. The collaboration between the platoon commander and the second in command is likely to be more effective when the natural tendencies towards either a robust or agile approach are opposite. In that case, they will complement each other and perform leadership collectively. Another form of collective leadership emerges when a member of the platoon develops leadership influence with his approach based on knowledge and experience from a previous mission. For example, when another commander of an IFV brings the conflicting viewpoints (creative deployment versus communication risks) together in a new technological advanced idea that works in practice and is far less risky, and discusses this idea with his peers to gain support and subsequently with the platoon commander. He clearly sees the benefits of both the proposed agile approach and the proposed robust approach, and is capable of consciously combining them in a balanced both robust and agile approach for the situation at hand. In this case, the IFV commander performs ambidextrous leadership. The platoon commander may support or reject the idea (and the leading influence of the commander of the IFV) by matching it with his own insights, thoughts and views. Depending on the decision of the platoon commander, the emergent, ambidextrous leadership of the commander of the IFV will be rejected or accepted.

Parent organisations that are hierarchically structured and organised, will often apply ambidextrous leadership, more specifically enabling leadership and an emphasis on operational leadership over entrepreneurial leadership when contributing to NetForce with specific capabilities (nodes). However, there are situations and contexts in which parent organisations need to emphasize entrepreneurial leadership over operational leadership. Enabling leadership is needed to make sure that the emphasis is in line with the requirements of the context. Ambidextrous leadership in parent organisations will mainly manifest as single appointed leadership, because many organisations are hierarchically structured and organised. Collective, often informal, manifestations alongside overall decision-making authority and control by single, formal managers or commanders are possible when based on expertise, knowledge and skills.

Single, appointed ambidextrous leadership
often with emphasis on operational leadership

In **NetForce collaborations** like temporary sub-networks, orchestrating elements and a strategic coalition, ambidextrous leadership - more specifically enabling leadership and an emphasis on entrepreneurial leadership over operational leadership - is an essential quality for (emergent) leadership. However, when the collaboration or context requires the emphasis needs to switch to operational leadership over entrepreneurial leadership. Enabling leadership needs to make sure that the leadership emphasis is in line with the requirements of the context. Because leadership in NetForce collaborations will often emerge in the social process of ad hoc collaboration, it is very likely that leadership will be manifested as emergent collective ambidextrous leadership based on specific expertise, knowledge or skills. Leadership functions may be distributed between different participants or shared with all participants in the collaboration. However, single leadership remains possible when the participants in NetForce collaborations choose to do so and agree upon the implications.

Emergent, collective ambidextrous leadership
often with emphasis on entrepreneurial leadership
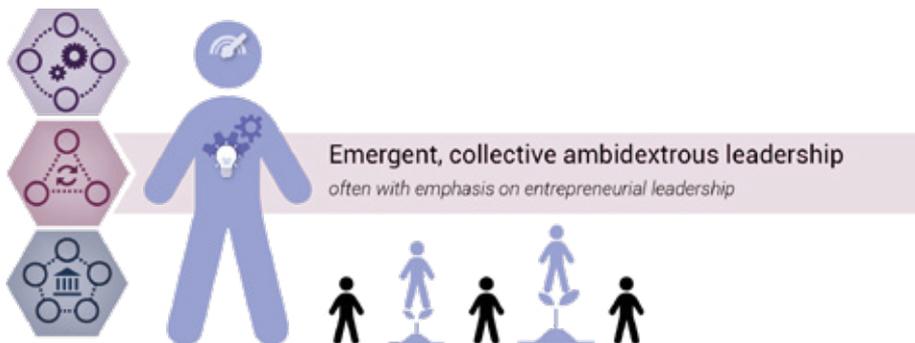
Concluding remarks

Ambidextrous leadership, enriched with the three forms of leadership in the complexity leadership framework (operational, entrepreneurial, and enabling leadership), and different types of single and collective leadership form an essential, connecting element of the overall NetForce Command concept. In chapter 4 you can read how ambidextrous leadership and collective leadership become visible in the three archetypes and how they are connected to self-synchronisation and orchestration and to the concepts developed for decision-making and information management. Ambidextrous leadership and collective leadership have implications for military nodes and the armed forces in general. In chapter 6 we provide a broad overview and analysis of the implications along the DOTMLPFI[24] lines, which are essential factors for developing and implementing the capability NetForce Command. More information on ambidextrous leadership, complexity leadership and collective leadership can be found in the further reading suggestion below.

Further reading

Bemmel, I.E. van & Boor, R.A.E. van der (2019). V1604 Leadership in NetForce; concept for leadership in complex, dynamic and networked environments. TNO report: TNO 2018 R11308, Soesterberg: TNO.

---

24. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

Watch the explanimation Decision-
Making in NetForce
www.tno.nl/netforcecommand

3.4   Decision-Making in NetForce

Because control is (almost) impossible in complex, dynamic and networked environments, agile approaches are required. An agile approach means performing relatively small interventions to influence the mission environment into a desired direction and adapting those interventions when the environment does not seem to bend towards that desired direction. In other words, an agile approach means using an incremental or iterative process to influence the mission environment and realise effects. An agile approach does not mean pursuing every opportunity and it does not mean working without a plan either. It means working with a strategy that emerges gradually.

The effectiveness of an agile approach strongly depends on the situational understanding of (specific situations in) the complex, dynamic mission environment, the ability to learn from interventions and the ability to quickly adapt or develop new interventions to influence that environment. An agile approach requires another approach to planning and decision-making than most organisations use. Most organisations that are hierarchically organised and structured, apply centralised decision-making: decisions are made by the top layers and based on robust planning. However, centralised decision-making is not likely, nor possible in a NetForce that consists of multiple actors that do not function in one hierarchical chain of command, but collaborate in temporary sub-networks and orchestrating elements. What approach to decision-making is likely to emerge in nodes? And what approach to decision-making is likely to emerge in NetForce collaborations like temporary sub-networks and orchestrating elements?

From schema oriented to (social) constructivist and social influence oriented decision-making

An agile approach requires a shift from a schema orientation to decision-making to a constructivist and social influence orientation to decision-making. A schema orientation to decision-making presents decision-making as a structured, step-by-step, task-oriented process (Chahine et al., 2017). Especially in the armed forces, there are many examples of a schema orientation to decision-making, for example the Military Decision-making Process (MDMP), the Comprehensive Operations Planning Directive (COPD), the seven questions model, and specific procedures like SALTA's[25] and 9-liners. Schema orientations provide a systematic approach towards decision-making by dividing the decision-making process into several neat steps (or heuristics) to be followed.
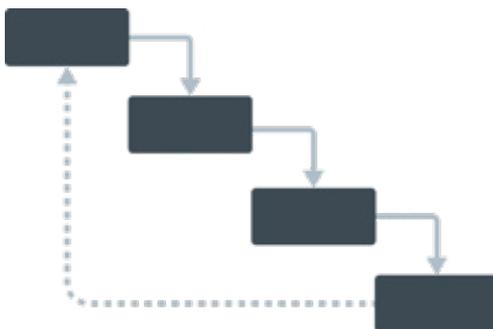

Figure 22 Schema orientation to decision making

---

25.   S: Size; A: Activity; L: Location; T: Time; and A: Actions.

For some contexts, this is very effective, for more complex and dynamic contexts it will often be less effective. One can compare schema orientations in a complex context with a chess player who fixes on a path to checkmate in 25 moves before the game has even begun, to find out it will not work after his opponent has made a few moves. Strangely, we still hang on to this intricate way of planning and decision-making, disregarding that people and groups do not (always) make decisions in a well-ordered fashion, accepting that schema oriented decision-making costs (too much) time and disregarding that contexts change continuously and no plan survives first contact. Furthermore, schema-oriented decision-making assumes that optimal situational awareness and understanding are possible, while in practice the mission environment is too complex and dynamic to attain full situational awareness and understanding, let alone shared situational awareness and understanding. Also, schema-oriented decision-making can mean that chances and opportunities in the dynamic environment remain unnoticed.

The constructivist orientation to decision-making fits better with an agile approach, because it is based on the idea that groups construct an understanding of (specific situations in) the environment, the tasks, the group, and the group members, through collective information processing (Chahine et al., 2017). This processing involves an active search for understanding in which incoming experience is reorganised and integrated with existing knowledge. This iterative and ongoing process of creating situational understanding which will never be finished or complete, is important when applying an agile approach. Constructivist orientations differ from schema orientations as they focus on the group's construction of their understanding, instead of focusing on the specific steps that groups follow during the decision-making process.
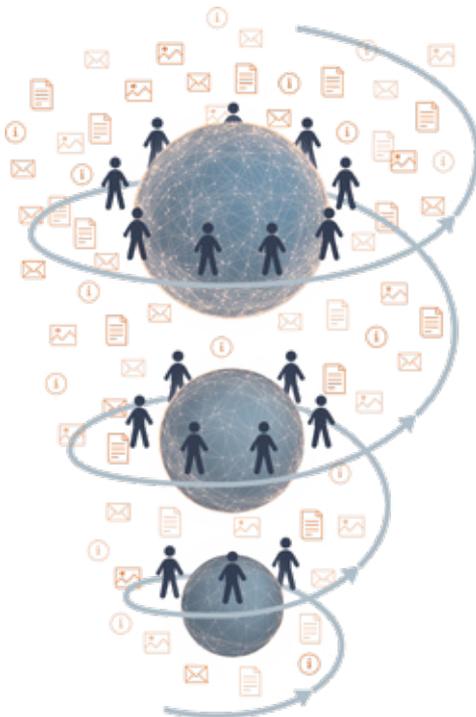
Figure 23 Constructivist orientation to decision-making

Furthermore, an agile approach in NetForce is only effective when decision-making gives room for the social interaction dynamics in NetForce (see section 2.3) and contributes to harmonisation of efforts. This focus on social interaction dynamics corresponds with social constructivism and the social influence orientation to decision-making. According to social constructivism, reality is not based on objective facts, but on interpersonal interaction and agreement on what is real (Cottone, 2001). Social constructivism takes decision-making out of the cognitive domain and places it into the social domain, stating that all behaviour is biologically affected and emerges through social interactions (Cottone, 2004). According to social constructivism, knowledge is not something in people's heads, but something people develop together (Cottone, 2001). Thus, a decision is "simply an action taken within a social context deriving from biological and social forces" (Cotton, 2004, p. 7). Social constructivism goes well with the social influence orientation to decision-making, which focuses on how group members influence each other and how group discussions influence and alter the group's viewpoint on a decision (Chahine et al., 2017). Social influence is based on the idea that decisions in groups may not be as neatly organised as they are conceptualised in schema orientations, nor may they have a shared and coordinated effort to produce the best decisions as conceptualised in the constructivist orientation.

Figure 24 Social constructivism and the social influence orientation to decision-making

Applying a combination of the constructivist, social constructivist and social influence orientation to decision-making will enable NetForce nodes to implement an iterative and agile approach. Tactical Designing and Interorganisational Negotiation are processes to operationalise these orientations to decision-making in NetForce.

Tactical Designing

Tactical Designing is an iterative process that supports decision-making in complex, dynamic and networked environments and provides an alternative for the often linear process of design, planning and execution. Tactical Designing seems a paradox, because design is often applied as a strategic planning process enabling decision-making on a strategic level and resulting in a strategy that provides guidance to lower levels. However, when studying design theory (Zweibelson, 2015), it becomes clear that design is meant for coping with complex, dynamic environments. When applied well, design begins and ends with clear iterations of a strategy and never results in a strategy that exactly describes how to achieve objectives from start to finish. A design is something that emerges, not a campaign or a strategic plan that can be developed in advance. Most organisations are however hierarchically structured and organised and, often unconsciously, turn design into a schema oriented process for the development of a strategic plan that enables them to control, correct and align their core business (Zweibelson, 2017). By applying design in this way, it is not useful for coping with complex, dynamic mission environments.

Tactical Designing means that strategies to cope with the complex, dynamic and often networked mission environment are emerging iteratively in the field. There are several examples of strategies that emerged iteratively in the field during the Netherlands ISAF mission in Uruzgan: working with patrol bases to increase influence and presence in a certain area; enhancing the relationships between security partners by creating an official community of Big 6 security partners; or stimulating social cohesion in communities to enhance economic prosperity. Full understanding of the environment is almost unattainable and always temporary. This implicates that nodes, temporary sub-networks and orchestrating elements plan and execute their specific activities based on a purpose and a general, often incomplete strategy (tactical design) which is based on their current, often partial understanding of the environment. A more thorough understanding of the environment is gained incrementally by acting in that environment in line with their general idea or strategy (tactical design), by monitoring changes in the environment, which may or may not be caused by own activities, and by analysing and integrating the perceived changes into an improved understanding of the environment. This means that elements in NetForce move from the known into the unknown aspects of the environment, thereby slowly reducing the unknown aspects and increasing situational understanding. NetForce elements switch their tactics or their strategy towards a purpose when their improved situational understanding gives a reason to do so. This continuous process of doing, probing, learning and adapting in a complex, dynamic and networked mission environment, we call Tactical Designing.

The process of Tactical Designing is similar to a method called Liberating Strategy (McCandless & Schartau, 2018). A liberated approach to strategy is 'a middle path between the single monolithic (over-controlled) and the "no plan" (under-controlled) extremes of strategy making' (McCandless & Schartau, 2018, p. 3). When applying a liberated approach to strategy in NetForce, control is distributed to all elements in NetForce, which means that direction and unity of effort are created by the elements in NetForce that share a common purpose.
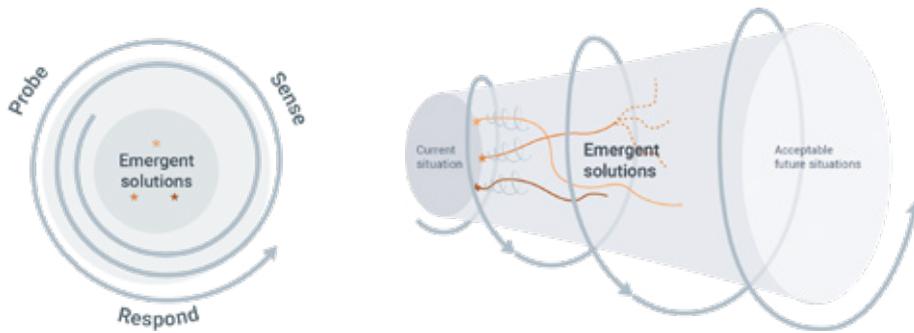
Figure 25 Tactical designing

Liberating Strategy has the following characterisations (McCandless & Schartau, 2018):

• The method includes and unleashes all relevant elements in NetForce to have influence and agency by using Liberating Structures. These are 33 practical methods that make it possible to include and engage all participants and require no training in advance.[26]
• The method is grounded in the present. Participants act-and-sense their way forward as strategy is mutually shaped in the moment. Because the acting-and-sensing approach is distributed and linked to a shared purpose, strategy-making can be infused into current activities.
• The method continuously reacts, probes, invents, evaluates, and shapes at the same time.
• The method relies on surprise and plans for serendipity. It does not rely on the past as proxy for the future. That seems controversial, but in practice chances and opportunities may arise unexpectedly and will often not be noticed when applying schema oriented approaches to decision-making.

Liberating Strategy or Tactical Designing (in military context) can be supported by **Strategy Knotworking** (McCandless & Schartau, 2018): a dynamic, iterative and adaptive way of planning. It consists of six core questions (McCandless & Schartau, 2018) that can be used between nodes and within temporary sub-networks and orchestrating elements:

1. Collective Purpose: What is the fundamental justification and deepest need for our work?
2. Context: What is happening around us that demands creative change?
3. Challenge: What are the paradoxes we must face in order to make progress?
4. Baseline: Where are we starting, honestly?
5. Shared Ambition: Given our purpose, what seems possible now?
6. Action and Evaluation: How are we acting our way toward the future, evaluating what is possible as we go? (Portfolio of investments as separate topics and as an interrelated whole.)

---

26. Liberating Structures add 33 more options to the five conventional approaches: presentations, managed discussions, open discussions, status reports and brainstorm sessions: http://www.liberatingstructures.com/ls-menu/

Answering these questions is a non-linear process that leads to a strategic narrative or a tactical design that is owned and operated by everyone, but can also be changed when new information becomes available. The answers are interrelated and slowly develop into a narrative about the starting point and a general strategy for moving forward. Shaping answers together leads to ownership, trust, and momentum for action (McCandless & Schartau, 2018). Liberating Strategy or Tactical Designing provides an alternative for the often very linear character of the process of design, planning and then execution in most organisations. With an emerging strategic narrative or tactical design, decisions on the planning (who does what, when, where, how etc) and execution of specific activities can be done more easily, less linearly and in harmony with other elements in NetForce.

Liberating Strategy or Tactical Designing can be applied in an interorganisational context, between nodes and within NetForce collaborations like temporary sub-networks, orchestrating elements and maybe even within strategic coalitions. A consequence of the interorganisational context is that representatives of the nodes are all influenced by the ambitions and interests of their respective parent organisations (authority ties, see section 2.3). Furthermore, (representatives of) these nodes will also have to cope with the influence of other ties: mutual influence ties, network ties, orchestration ties and strategic influence ties (see section 2.3). In accordance with the social constructivist and social influence orientation to decision-making, this means that decisions in NetForce collaborations will often be preceded and influenced by negotiations between (representatives of) participating nodes. In the next section we explain how decisions in these NetForce collaborations are negotiated.

Interorganisational Negotiation

Elements in NetForce are implicitly or explicitly involved in different types of (negotiated) decisions. On the one hand, decisions may relate to interactions with other elements in NetForce (decisions about interaction process) and on the other hand, decisions may concern tactical designing, including the planning and execution of specific activities (decisions about content). The first type, decisions about interaction, easily relate to the four phases of ad hoc interaction and collaboration: positioning, shaping, executing and transforming (see section 2.3). Decisions concerning the positioning phase include the need for interaction and the type and level of interaction. Decisions concerning the shaping phase include the interaction itself, especially the collaboration and integration in terms of function and purpose, composition, organisation and structure, culture and behaviour. In the executing phase, decisions relate to the (intensity of) interaction during the execution of activities. Lastly, decisions concern the transformation of the interaction. Decisions related to interaction with other elements in NetForce have influence on decisions about content, for example the tactical designing and the specific activities to be executed. Furthermore, both types of decisions are influenced by the maturity of the interaction and by the developments in the mission environment.

The negotiation between nodes, temporary sub-networks, orchestrating elements and strategic coalitions will often have an interorganisational character, because different parent organisations will be represented in these negotiations. Interorganisational Negotiation is seen as a process by which organisations with different backgrounds, interests and objectives, experience some kind of interdependence in realising desired effects and seek to be more effective through jointly agreed action (Mouzas & Ford, 2003). Interorganisational negotiation in NetForce is important because elements in NetForce are influenced by other elements in NetForce via multiple ties (see section 2.3). To protect and follow own interests, each element in NetForce needs to negotiate with

other elements in NetForce. Because there are no hierarchical command and control relationships to structure and organise harmonisation, and because collaboration and commitment of other elements is not a given, especially not in an environment that changes continuously, negotiation is needed to unleash the power of existent and often hidden connections and alternatives (Mouzas & Ford, 2003) in a NetForce.

In NetForce each element (node, temporary sub-network, orchestrating element or strategic coalition) has multiple dyadic negotiations in a web of different types and levels of interactions and relationships (see section 2.3). These dyadic negotiations have influence on other dyadic negotiations, interactions and relationships in NetForce. Mouzas & Ford (2003) developed a model consisting of three phases of network negotiations. These three phases represent the mechanisms of negotiating in NetForce, which can take place in all four phases of ad hoc interaction and collaboration:

1. **Initiating real and actionable options**: in this negotiation phase the space of negotiation is influenced by the developments in the context, the resources and potentials of own and other elements in NetForce, the surrounding network and the parent organisations that are involved via the (representatives of) nodes. The negotiation space is often implicit at the beginning of a negotiation and becomes more visible during the course of a negotiation. This is visualised in figure 26. The way organisations use this negotiation space is described in the next two phases of the model.
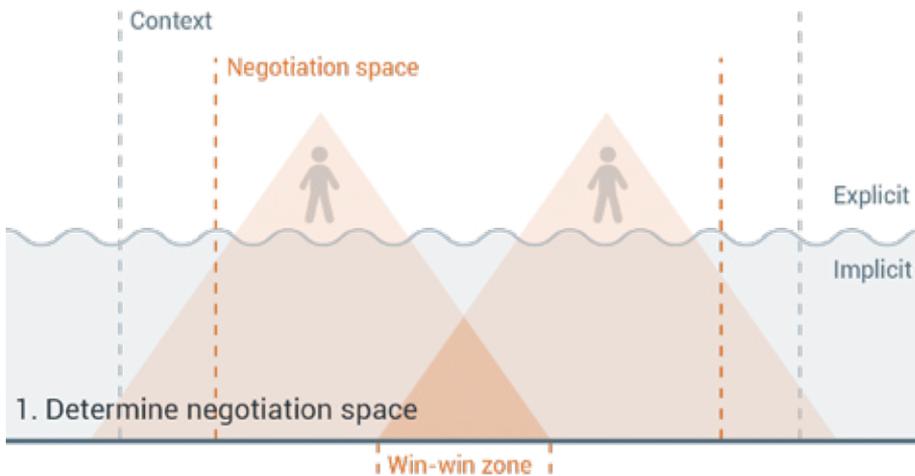

Figure 26: Determining the negotiation space and the space where a mutual gain can be realised.

2. **Infusing options into interactions and relationships**: in this negotiation phase implicit negotiation is followed by more explicit negotiation about:

- **Proposals and issues**
  Proposals can take the form of suggestions for collaborative projects or suggestions for exchange of information, resources etc. Proposals can bring specific issues to the negotiation table like quality, prices etc. and often entail underlying interests;
- **Interests and stances**
  Stances in negotiated issues are often explicitly stated; underlying interests often remain implicit, hidden, or not expressly formulated;
- **Retaining and adapting options**
  Options can be expanded, modified, or restricted during the course of a negotiation.

In practice, infusing options into interactions and relationships in NetForce takes the form of providing the rationales and the resources that enable other elements in NetForce to initiate change. This is visualised in figure 27.
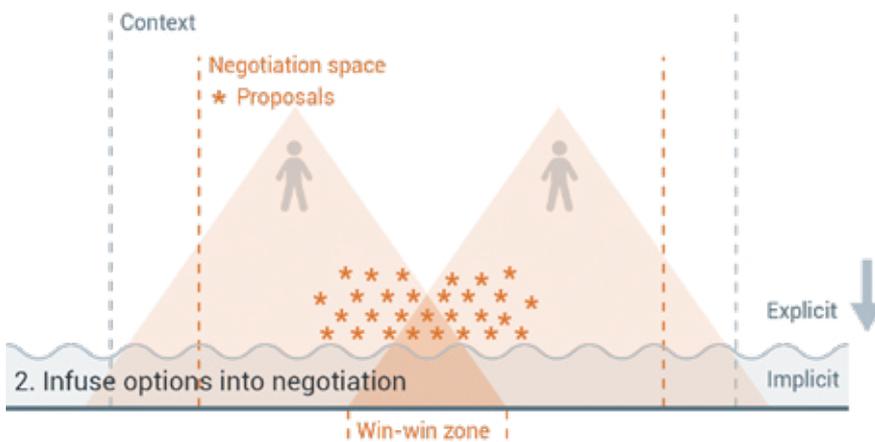

Figure 27: infusing option into the negotiation

3. **Realising wise trades:** in this negotiation phase it is all about reasonable trading opportunities for mutual gain as visualised in figure 28. To realise wise trades, it is necessary to differentiate between the following:

- **Negotiated deal and Alternative options**
  A deal is possible when the negotiated agreement is better than alternative options. Awareness of these alternative options is therefore conditional for crafting a deal that is beneficial for all elements involved in the negotiation. Furthermore, perceived alternative options may change during the course of a negotiation;
- **Creating value and Capturing value**
  The possibilities to create joint value drives negotiation between elements in NetForce. However, decisions about sharing the created value drives another negotiation in which it is important to balance between the short term value of a deal and the long-term value of a relationship;
- **Playing the game and Changing the game**

In NetForce negotiation is a game with rules that are implicitly shared between the elements involved in negotiation. During negotiation the rules of the game are also challenged and changed based on underlying interests and different weights on concerns with potential deals.
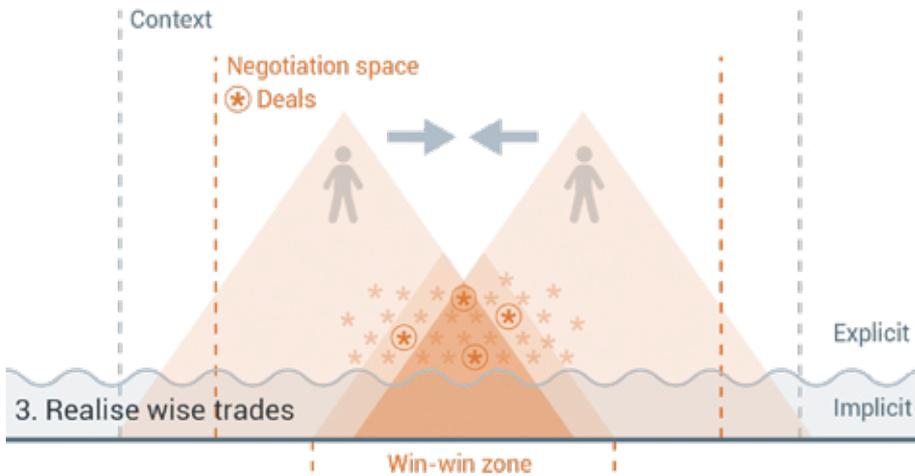
Figure 28: realising wise trades through negotiation

Interorganisational negotiation is linked to complex, dynamic and networked environments and the availability of alternative options in these environments. Because in these environments most elements are dependent on the resources and actions of other elements in NetForce, most of the decisions related to these activities in NetForce are negotiated.

Preconditions for decision-making in NetForce

In NetForce we envision that Tactical Designing or Liberating Strategy, including Strategy Knotworking, will provide an alternative for decision-making in military and civilian nodes and in NetForce collaborations that function in complex, dynamic and networked environments. Furthermore, in these mission environments, Interorganisational Negotiation is needed to unleash the power of existent and often hidden connections and alternatives in NetForce. There are several preconditions to make Tactical Designing, Liberating Strategy and the increasing role of Interorganisational Negotiation possible in NetForce and to ensure that it contributes to a balanced and effective agile approach. These preconditions are empowerment, self-assessment and harmonisation.

Empowerment implies that parent organisations give autonomy and freedom to their nodes to decide and act in line with the dynamics of the environment without going up the chain of command. **Empowerment means power to the edge of an organisation** (to the nodes, temporary sub-networks and orchestrating elements), where the organisation interacts with the mission environment to have an impact or effect on that mission environment (Alberts & Hayes, 2003). Empowerment also implies (more) authority and responsibility at the edge and therefore the demand of more experienced and skilled personnel at the edge. Furthermore, empowerment implies a changing role for parent organisations. Parent organisations should be focused on enabling and supporting their nodes with the execution and sustainment of activities. However, many hierarchical organised and structured parent

organisations will also be inclined to provide the nodes with information, constraints and restraints related to their own ambition, vision, objectives and policies. That information may be beneficial for the nodes, but it may also lead to too much control. When there is too much control by the parent organisation it will impair the nodes in contributing effectively to NetForce and in coping with the complex, dynamic and networked environment. In other words, managers/commanders of parent organisations need to prevent rigidity, micromanagement and control, because that will probably be highly counter-productive for the nodes that operate in a complex and dynamic environment. It will make the nodes less adaptive, because the approach of their parent organisations will not match with the approach needed in the environment and thus create tension. Therefore, parent organisations should focus on providing maximum support (for example specific and tailored training and education, solid clothes and materials, finance of projects, experts, etc) to the nodes, but also to the temporary sub-networks, orchestrating elements and strategic coalitions, in which their nodes are represented. In general it is expected that the influence of parent organisations will be more present in archetype B via the orchestrating elements and even more substantial in archetype C via the strategic coalitions.

Self assessment is the ability to enable all elements in NetForce to be aware of, consider and cope with external influences when planning and deciding on courses of action or specific activities. It is the ability that ensures that the elements in NetForce function in harmony with each other's actions and intentions. According to the Multinational Capability Development Campaign (MCDC) Information Age Command And Control project (2017 and 2018), self-assessment consists of activity assessment and capability assessment.

Activity assessment

Activity assessment focusses on the types of activities that can be done and on the relative priority of those activities for that specific moment or situation. When applying tactical designing or liberating strategy, insight in possible activities to execute is important for the decision on what to do (courses of action). Types of activities can vary between an immediate request for cooperation by another node or a response to an acute crisis situation to a level of 'wheel and deal' or a contribution to strategic goals of the parent organisation. Activities can be executed by the node itself (with or without capacity support[27]) or might require a request for cooperation. The relative priority of an activity is amongst others influenced by the type of activity. For example, a response to an acute crisis situation will often be more time critical than a contribution to a strategic goal, and might therefore receive a higher priority. Next to the type of activity the following assessments should also be taken into account:

- Assess the expected impact of the activity, or the consequences when the activity is not performed;
- Assess whether the activity is time critical (can it wait or is now the opportunity);
- Assess the 'costs' (and opportunities) of ending ongoing activities;
- Assess the longer term influence on own capabilities (sustainability);
- Analysis of the impact of the decision/action regarding own as well as other actors' intentions and/or contributions.

27. Capacity support refers to the temporary exchange of a capacity from one node to another node, without collaboration on the use of the capacity. Examples are the temporary use of a truck or a specific tool or system.

Capability assessment

Capability assessment provides information on whether the activity can be performed by itself (with or without capacity support), or if collaboration is required. Capability assessment concerns performance information on one's own capabilities. Once assessed the performance can for example be indicated on a 5 point scale; very high (80 – 100%) – high (60 – 70%) – moderate (30 – 50%) – limited (0 – 20%). When capabilities are limited, (immediate) capacity support is needed to continue with the activity. 'Moderate' indicates that capacity support is needed soon. 'High' indicates no capacity support is needed and 'very high' indicates a surplus of capabilities for the activity. Capacity support can be seen as a limited form of collaboration in NetForce. Depending upon the capabilities of a node, most nodes within a NetForce will sooner or later need capacity support to perform activities. But nodes cannot command other nodes to provide them with a certain capacity, they must persuade or seduce other nodes to support their activity. When the intended activities cannot be executed with own capabilities (even with capacity support), more intense cooperation with other nodes is needed. This might even lead to the formation of a temporary sub-network.

Focus on harmonisation. To unleash the power of a NetForce consisting of military and civilian nodes, and several temporary sub-networks, orchestrating elements and strategic coalitions, in which different parent organisations are represented, it is essential for all elements in NetForce to negotiate and to focus on reasonable trading opportunities for mutual gain. Especially in complex, dynamic and networked environments in which it is almost impossible to realise objectives and create effects solely. A focus on harmonisation is essential because nodes do not have the mandate to control other nodes, and temporary sub-networks and orchestrating elements can only influence, not command and control the nodes. Harmonisation is about finding common ground and utilising the strengths in the NetForce. A focus on harmonisation means openness towards shaping the interaction and collaboration (or even integration) in terms of composition, organisation and structure, culture and group behaviour (see section 2.3). Openness implies, amongst other things, the ability to leave one's comfort zone, to take on other roles, and to accept that the way of working will be different than in the own organisation. A focus on harmonisation also means respecting other's point of view, ambition, interest and culture. When all elements in NetForce focus on harmonisation in their decisions during interactions and collaborations, it becomes possible to create unity of effort and to perform a balanced and effective agile approach to cope with the complex and dynamic mission environment.

Concluding remarks

Tactical Designing, Liberating Strategy, including Strategy Knotworking, and Interorganisational Negotiation are decision-making concepts that need to be included in the overall NetForce Command concept, because these concepts can enable self-synchronisation, orchestration, leadership and collaboration in NetForce. In chapter 4 you can read how Tactical Designing, Liberating Strategy and Interorganisational Negotiation become tangible in the three archetypes and how they are connected to self-synchronisation and orchestration and to the concepts developed for leadership and information management. The concepts for decision-making have implications for military nodes and the armed forces in general. In chapter 6 we provide a broad overview and analysis of the implications along the DOTMLPFI[28] lines, which are essential factors for developing and implementing the capability NetForce Command. More information on Tactical Designing, Liberating Strategy and interorganisational negotiation in NetForce can be found in the further reading suggestion below.

Further reading

Bemmel, I.E. van, Eikelboom, A.R. & Hekken, M.C. van (2019). V1604 Decision-making in NetForce; concept for decision-making in complex, dynamic and networked environments. TNO report: TNO 2018 R11309, Soesterberg: TNO

---

28. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
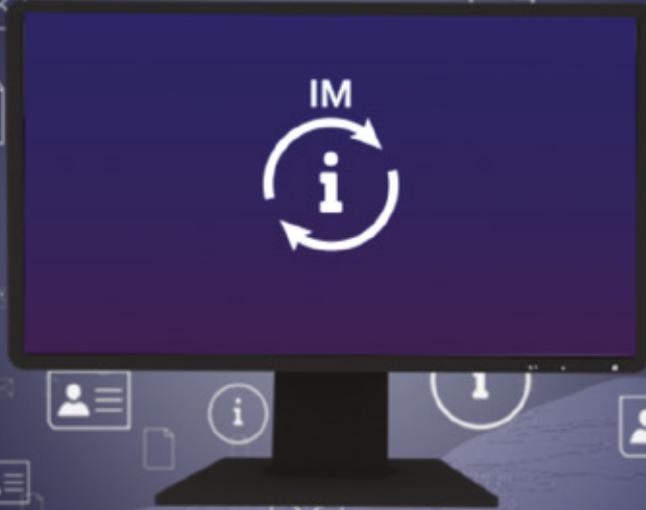
Watch the explanimation Information
Management in NetForce
www.tno.nl/netforcecommand

3.5 Information Management in NetForce

Having the right information with the right quality at the right time and the right place for the right person has always been an important prerequisite for military operations. But the challenges to fulfil this prerequisite have only increased. Already for decades the amount of information that we are dealing with grows exponentially. Both the number of potential sensors of information and the capabilities of these sensors augment continually. To deal with this increasing amount of sensors a capability to manage the information is paramount. But the amount of information is not the only problem. The complex, dynamic and networked mission environment (as described in section 1.1) also introduces unpredictability of information needs for the various actors that contribute to achieving mission objectives. Even if we would be able to collect, process and store all the available information in a 'managed' way and therefore would be able to track down this information when needed, it still would be very difficult to determine the 'when needed' part of this condition within the time constraints of the mission. In NetForce this unpredictability not only applies to the content of the information needs, but also to the nodes that will have the information needs. As described in chapter 2, in NetForce nodes will appear and disappear, temporary sub-networks will be formed and dismantled, nodes will join and leave temporary sub-networks, and so on. Determining the right place and person, i.e. the right recipient of the right information, is therefore also a huge challenge in NetForce.

Which variants of information management can be distinguished in NetForce and what are possible conceptual solutions for these variants? More specifically: How can nodes discover each other, in order to meet their mutual information needs? How do nodes notify which information they have available and how can they express their information needs? How can nodes make agreements with each other about the exchange of information (what and how?)? How can the progress and the quality of the actual information exchange be assessed and how can the information exchange be intervened when necessary?

The Information Management function and the plan-based approach

As stated in the introduction the objective of Information Management (IM) is to provide the right information with the right quality at the right time and the right place for the right person. Information is recorded, processed, stored, retrieved, used, exchanged, and, at some point in time, archived or destroyed. This process is called the Information Life Cycle. In order to meet the objective, Information Management will try to optimise the Information Life Cycle. This is depicted in figure 29.
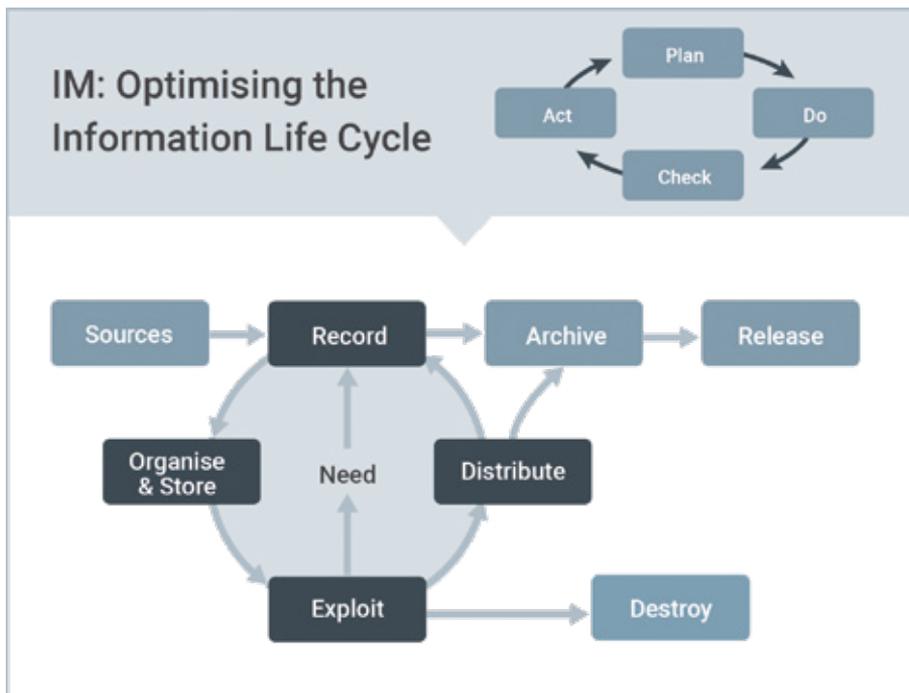
Figure 29 Optimising the Information Life Cycle

In optimising the Information Life Cycle to provide the right information with the right quality at the right time and the right place for the right person, Information Management consists of the following main functions:

- Recording and advertising information needs and information availability of the different involved actors/nodes;
- Managing the actual recording, storage, processing and exchange of the information itself: the Information Life Cycle;
- Ensuring the ability to find relevant (information providing) actors/nodes and types of information;
- Determining the status and progress of the Information Life Cycle in relation to the information needs, and, if necessary, adjusting elements of the Information Life Cycle.

Today, many organisations, including the Netherlands Ministry of Defence, are still in the process of setting up, organising and developing an Information Management capability aimed at an optimal Information Life Cycle within their own organisation. Usually a Plan-Do-Check-Act approach is leading for this Information Management capability.

This approach is based upon the creation of an IM plan for the optimal design of the Information Life Cycle within an organisation. An important part of the IM plan is predetermination (as far as possible) of the information needs of the various actors (as producer and consumer of information) within the organisation, including associated quality requirements. Then, the information channels that will be used to support that information (exchange) need are also determined and designed in advance. This is the Plan-part of the Plan-Do-Check-Act approach.

The IM plan leads to the daily activities that must be carried out in the context of Information Management:

- Performing support activities for activities of the Information Life Cycle, based on the IM plan (Do).
- Monitoring the status and progress of the Information Life Cycle in the organisation, specifically focused on possible bottlenecks / problems, which necessitate adjustments (Check). This monitoring is based on 'management' information, like:
  - Indicators that information is produced and published, but not or rarely used.
  - Indicators that information is needed, but barely available.
  - Indicators for the degree information is available on time for the right nodes and suffices the 'quality' needs of that node (in terms of actuality, correctness, etc.)
  - Indicators for the degree similar information is stored at different locations and the degree of inconsistency.
  - Etc.
- Implementing possible adjustments or structural improvements in the Information Life Cycle, based on the monitoring (Act). Examples of adjustments or structural improvements are:
  - Restructuring the stored information within one or more information channels. 'Cleaning up' information that is stored at different locations, to reduce or prevent inconsistencies.
  - Setting-up new or reconfiguring existing information channels, to make them more suitable for the desired information exchange.
  - Taking measures to increase end user awareness to, for example, publish and store information at the right location at the right time.
  - Etc.

A possible way of working for the Netherlands Ministry of Defence based on the Plan-Do-Check-Act approach is described in the IMnibus (Benda et al., 2014). Adopting the Plan-Do-Check-Act approach on Information Management is a good first step to develop an Information Management capability within organisations and to 'get a grip' on important Information Management issues. As stated earlier, many organisations are in the middle of this development. However, the unpredictability of both the complex, dynamic mission environments and the dynamic, networked and JIMP way of working in NetForce to cope with these environments, also requires a more dynamic, emergent approach towards Information Management (with conservation of the useful elements of the Plan-Do-Check-Act approach).

The next step: emergent information sharing and management

In fully self-synchronising variants of NetForce (archetype A), there will be no coordinating Information Management entity beforehand, meaning that the Plan-Do-Check-Act approach, described in the previous section, will not apply. Still, the main IM functions (Recording and making known information needs, Managing the Information Life Cycle, Ensuring the retrievability of information, Monitoring status and progress of fulfilling the information needs) have to be produced by the individual nodes and temporary sub-networks in a more emergent way.

At first, nodes will try to obtain and manage information on their own, until they acknowledge that their information position is insufficient. Nodes will search for information available at other nodes to augment and improve their information position. This requires that nodes are able to express their information needs and their information availability to other nodes. When there is limited to no digital support to express information needs and information availability, nodes will only be able to contact familiar nodes, face-to-face or by telephone, E-mail, etc. Through coincidence they will meet new nodes, but in general information available at 'unknown' nodes and information needs of 'unknown' nodes will remain unknown. As a consequence, this way of emergent information sharing will provide limited results (in terms of 'the right information, at the right place at the right time').

In order to obtain a higher degree of emergent information sharing within NetForce, a digital environment is needed in which *information profiles* of nodes (expressing what type of information a node needs and what type of information a node has available) can be shared between the nodes in NetForce. We refer to such an environment as a *digital information profile environment*. A basic form of this environment still requires nodes to fill in their information profile manually. Nodes must also express their available information (products), using metadata. In this *digital information profile environment* nodes will be able to search for available (types of) information. The search results will be a combination of contact data of nodes having these types of information and metadata of information (products) matching the search criteria. Besides active searching by nodes in this *digital information profile environment*, nodes might also receive suggestions for relevant nodes and/or information (products), based on the information needs expressed in their *information profile*.

When nodes have discovered each other's information needs and relevant information available at other nodes, they will start to make agreements on what information will be exchanged, which information channels will be used and which prerequisites or boundary conditions apply to an information exchange, based on the content and the security requirements of the information. Nodes might even decide to form a temporary sub-network to start a more structural information exchange with each other.

Today, many nodes will use 'basic' information channels like E-mail or a common fileshare. If nodes have worked together before, and have already shared information with each other, or if they decide to create a temporary sub-network, a more advanced shared digital platform may be set-up and used. This will be motivated by the risk that, otherwise, information will be exchanged by different information channels, possibly leading to inconsistencies in information at different 'places' (nodes). At the moment there are several technological developments to create 'richer' digital information sharing and collaboration platforms. We refer to this platforms as *digital information environments*. These *digital information environments* offer various communication patterns (synchronous – chat, skype, VTC, and asynchronous – sharepoint-like) combined with extended search possibilities, version control and 'smart cloud'-solutions to store information.

If a *digital information environment* and a *digital information profile* environment are combined, it will also be possible to search for information and receive suggestions for relevant information without the need to contact the 'source' node of this information. Of course, contact information of a 'source' node may still be relevant or even necessary, if the information exchange requires synchronous communication with or permission from this 'source' node. Combining the *digital information environment* and the *digital information profile* environment will also offer the possibility to create and update the

information profiles of nodes, based on their information search and publication behaviour. It is likely that the digital support mentioned above will be available at the time horizon in which NetForce operations are projected. Currently, the Netherlands Ministry of Defence is already experimenting (in a National Technology Project) with a Federative Digital Collaboration Environment (FeDiCE) and also contributes to the NATO Future Mission Networking (FMN) developments.

When the (digitally supported) information processing, storage and sharing (the Information Life Cycle) between the nodes, whether or not united in a temporary sub-network, has emerged as described above, it will be possible to generate and present 'management' information to the nodes. Examples of this 'management' information have been given earlier in this chapter. The possibilities for generating this 'management' information will be wider if there is an integrated *digital information environment* and *digital information profile environment*. If the information exchange is supported by loosely coupled, more 'basic' information channels, generating 'management' information will be more complex and less detailed, because a large diversity of crawlers (software to search within an information channel and retrieve steering information) will be needed. Generating 'management' information also depends on the possibility of nodes, having received and used information (products), to provide reviews or ratings on the usability of this information.

Generated 'management' information, presented at the nodes, may lead to one or more nodes starting to perform Information Management activities for a 'community' of nodes, whether or not united in a temporary sub-network. In that case a (subtle) transition to a more Plan-Do-Check-Act approach has been initiated: Information Management has emerged!

Required functionality of digital support

In the discussion above, numerous remarks were made about desired or even required digital support for information management, i.e. in optimising the Information Life Cycle to provide the right information with the right quality at the right time and the right place for the right person. We mentioned the combination of the *digital information profile environment* and the *digital information environment*, that would also provide digital steering information.

If we elaborate, we foresee that the following functionality would be required or desired:

- Publishing available information and automatic adding of labels (metadata) to this information. This does not only refer to administrative metadata (author, date, etc.) but also to metadata about the content of the information, using techniques like text mining, picture recognition etc. Of course, a user that publishes information must also be able to add labels manually. The user must also be able to choose whether or not to publish the information themselves or only the labels.
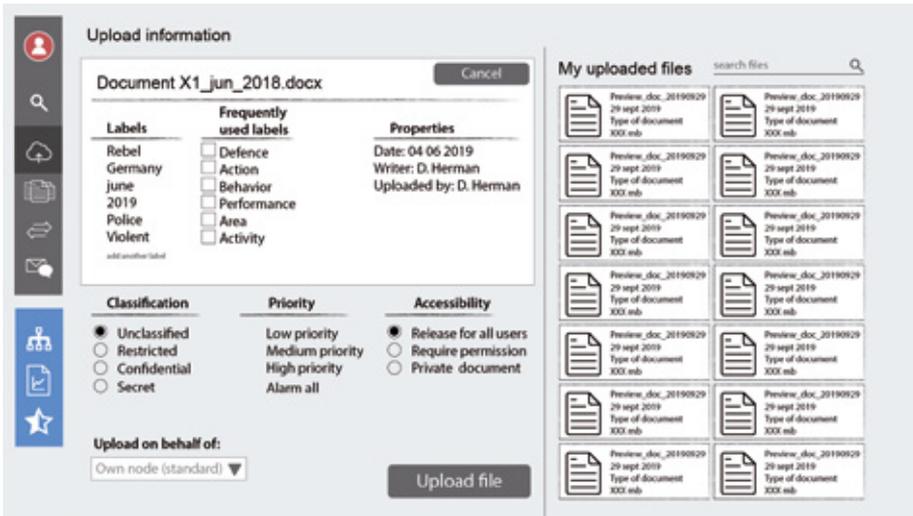
Figure 30 Screen to upload information and adding labels to the uploaded information

• Searching for available information using search criteria. These search criteria are matched with the metadata of available information and the matching results are presented. If the information itself was uploaded by the publisher and if the metadata of the information (related to security and risk) allow for direct release, then the user that performed the search operation will be able to use the retrieved results immediately. Otherwise, the publisher must be asked for permission to release the information. Apart from using search terms each time, this kind of support also allows for defining recurring search queries by a user. This user then will receive notifications every time information that matches a search query is published and/or changed.
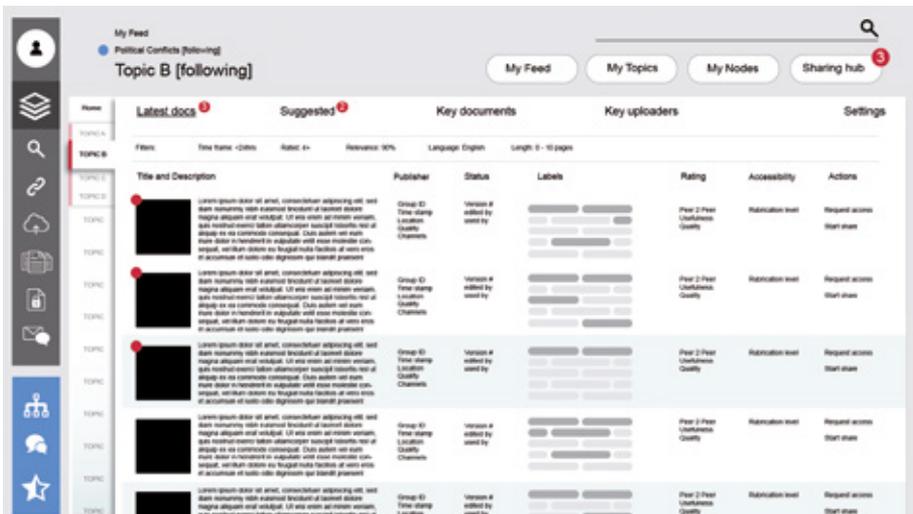

Figure 31 Screen which shows latest results or meta data (updates) on predefined search queries (either stated by the user or automatically deducted by technology).

- Automatic creation of information profiles (expressing the information needs of a user and the information that a user 'possesses') by using the search criteria and queries of a user and the metadata of the information that is published by this user. Once again, a user must also be able to update his or her information profile manually.
- Providing suggestions of potentially relevant information to users, based on the information profile of the users. Besides the notifications of new or changed information, these suggestions could also apply to possibly related information (not directly expressed in earlier search queries or in the information profile) or even to contradictory information, to prevent tunnel vision. This 'richer' way of providing suggestions would require semantic technology to relate terms, synonyms, etc.
- Determining suitable information channels for specific exchanges of information between nodes that cannot be supported by the 'usual' platform for publication and retrieval (e.g. for security reasons). Technology could determine which information channels would be suitable, based on the available channels of the nodes and based on the characteristics of the information (metadata). This also includes the 'choice' of a synchronous or an asynchronous information channel.
- Providing steering 'management' information about the current Information Life Cycle, both from an node perspective and from a network perspective. This could show (for instance):
  - who is using which information, how frequently and how well does it match the quality requirements of the users (timeliness, actuality, usability, etc.)
  - which information channels are used, how often, for what types of information and how good is the availability, capacity and the quality of the information channels
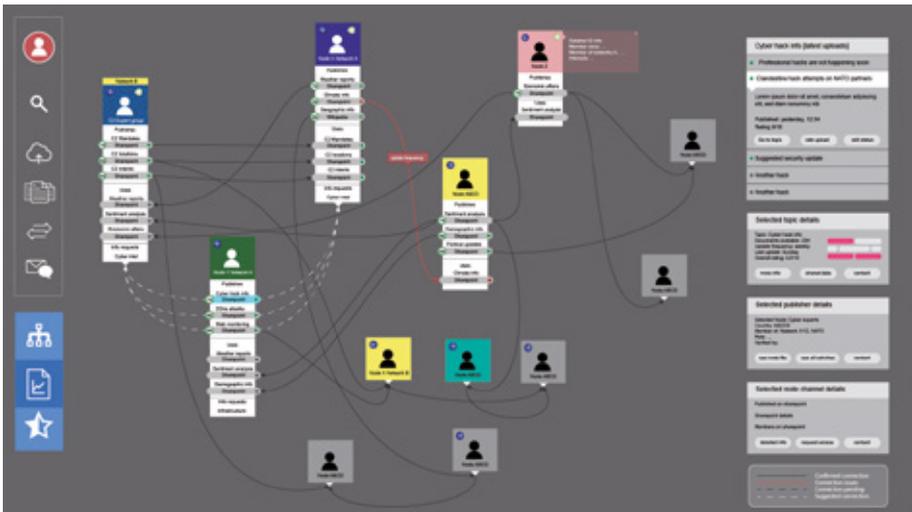

Figure 32 Screen showing the information exchange in the network (information content and quality view)

Note that the terms 'user' and 'publisher' that we used above may refer to any representative of a node or to dedicated information managers, dependent on the way the information sharing and management is organised. One should consider that the more extensive the information sharing and management is supported by technology, the more dependency on 24/7 availability of that technology is introduced. It is important that nodes always take fallback measures to retain some kind of information position for situations in which digital support is failing or absent. If a Plan-Do-Check-Act approach, with dedicated information management elements, has emerged or been set-up top-down, creating fallback measures will be promoted more pro-actively.

Outsourcing of Information Management?

When information exchange and a common Information Life Cycle between (a sub-network of) nodes, has been set up and when the transition to a more Plan-Do-Check-Act approach of Information Management is underway, a moment in time may be reached to consider outsourcing (parts of) the Information Life Cycle to specialised third-parties. For instance, the storage of information could be outsourced to a third-party that provides secure cloud-solutions. Note that if the Information Life Cycle is digitally supported to a large degree (the integrated *digital information environment* and *digital information profile environment* as described earlier), outsourcing takes the form of third-parties hosting the technological platforms that provide the integrated *digital information environment* and *digital information profile environment*. In fact, only the maintenance and sustainability of these technical platforms is outsourced in that case. The concerned third-parties do not interfere with the actual information content that is 'cycled' on these technical platforms.

One step, or perhaps a few steps, further would be to outsource the coordinating Information Management function to a third-party. In that case a third-party would get control over directing information flows, in other words determining which nodes receive which information. Of course, this would only work if all involved nodes have sufficient trust in this third-party. Furthermore, it requires that such a third-party has extended knowledge of the objectives, way of working, collaboration agreements, activities and associated information needs of the involved nodes. If these factors would be standardised and predictable and especially if the activities of the nodes would have a limited 'damage risk', third-party Information Management could be feasible. But, of course, in NetForce this is all quite the opposite. Especially the collaboration agreements, activities and associated information needs of nodes are highly dynamic and unpredictable. Therefore, completely outsourced Information Management in NetForce seems very unlikely.

It is worthwhile noting that the considerations stated above apply more strongly if there is limited digital support for Information Management. In that case, a larger part of the Information Management functions have to be performed manually by information managers, including decisions on which nodes receive what information. As discussed above, the fallback possibilities that a more manual Plan-Do-Check-Act approach of Information Management offers, are difficult to transfer to a third party, given the dynamic and unpredictable nature of collaboration agreements, activities and information needs.

If there is a 'rich' digital support (as described in the previous section) outsourcing Information Management is similar to outsourcing (parts of) the Information Life Cycle, which was discussed at the beginning of this section. The decisions on who receives and gets access to what information are then implemented in (rules within) the outsourced digital support platform, based on the information content that is provided by the users, without manual third-party interference. The stated concerns on outsourcing Information Management then only apply to the (fewer) remaining manual Information Management activities.

In summary, outsourcing is likely for technological, digital elements supporting the Information Life Cycle and the Information Management and unlikely for Information Management activities that relate to interfering with and directing the information content.

Manifestation of information sharing and information management in NetForce

Without extensive digital information sharing and information management support – in archetype A – information sharing between nodes will initially be based on familiar relationships and familiar information channels, which implies the risk that not all relevant information is available for all nodes. Depending on the duration of an interaction or collaboration between nodes, agreements on information sharing may change or some new information channels may be set-up. Note that this will only take place between nodes that are aware of each other's presence in the mission environment. When temporary sub-networks are formed, one or more representatives of the participating nodes might feel responsible for a more effective, efficient and coordinated way of information sharing. They will start to fulfil the role of an information manager and start to apply a more coordinated, plan-based, approach of information management within the temporary sub-network. It is unlikely that information management will arise between the temporary sub-networks. Information sharing between temporary sub-networks will remain to be based on familiar relationships and familiar information channels.

When there is rich digital support of information sharing and information management (the integrated *digital information environment* and *digital information profile environment*), broader information sharing between nodes and between temporary sub-networks will be enhanced. Moreover, the functional administrators of those digital support platforms will perform some Information Management activities (cleaning data, setting up and configuring new channels, etc.) and may, dependent on the need to back-up the digital support or to fill-in digitally unsupported gaps, also take on other (non-digital) Information Management activities.

In archetype B, it is likely that orchestrating elements may oversee the emergence of information management within and between sub-networks or may even appoint information managers. Dependent on the size and scope of an orchestrating element, the need for information management and implementing information management functions within the orchestrating element will also arise. It is also conceivable that information managers within an orchestrating element may perform information management for the nodes and sub-networks that are orchestrated by this element.

Concluding remarks

Having the right information with the right quality at the right time and the right place for the right person is a prerequisite for all the other NetForce Command concepts that have been described in this book. Information Management is the profession that must fulfil this prerequisite. And, because the information flows in NetForce will always be dynamic, complex and unpredictable, a 'traditional' plan-based approach of Information Management, although still a challenge itself in current operations, will not suffice. Emergent information sharing and management, a 'rich' digital support environment and possible outsourcing of information management are concepts that have to be explored and developed. In chapter 4 you can read how information sharing and management become tangible in NetForce and how they are connected to self-synchronisation and orchestration and to the concepts developed for leadership and decision-making. Concepts for information sharing and information management have implications for military nodes and the armed forces in general. In chapter 6 we provide a broad overview and analysis of the implications along the DOTMLPFI[29] lines, which are essential factors for developing and implementing the capability NetForce Command. More information on the information management function and the plan-based approach, emergent information sharing and management, including the required digital support and possibilities for outsourcing can be found in the further reading suggestions below.

Having the right information with the right quality at the right time and the right place for the right person is a prerequisite for all the other NetForce Command concepts

Further reading

Benda, R., Hekken, M.C. van, Pieneman, R. & Michel, M. (2019). V1604 NetForce informatievoorziening en informatiemanagement. TNO report: TNO 2018 R11566. Soesterberg: TNO.

Benda, R., Hekken, M.C. van, Pieneman, R. (2014). IMnibus – TNO Uitwerking van informatiemanagement binnen Defensie. TNO publication (in cooperation with Dutch Ministry of Defence). Den Haag: TNO

29. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

TOUR OF NETFORCE COMMAND

4

4   TOUR OF NETFORCE COMMAND

In chapter 1 and 2, we describe NetForce Command, explain that there are various implementations of NetForce Command on the scale from maximum self-synchronisation to maximum orchestration and that these implementations differ depending on the composition, the organisation and structure, and the interaction in NetForce. We also describe different aspects of group behaviour (NetForce Command concepts) that come out of the group dynamic process of social interaction in a NetForce: management and control (self-synchronisation and orchestration), leadership and followership, decision-making, and information management (see chapter 3).

To make NetForce Command more tangible, this chapter offers a tour of NetForce Command. Because there are infinite implementations, we chose three distinct (potential) implementations of NetForce Command to be able to study and describe NetForce Command: Emergent NetForce (archetype A), Emergent Orchestrated NetForce (archetype B) and Strategic Orchestrated NetForce (archetype C). These archetypes are explained in more detail in section 2.2. In this chapter we provide a tour of these three archetypes from multiple perspectives. Each tour consists of interviews with potential future actors and focuses on the potential functioning of NetForce Command in future complex, dynamic and networked mission environments. The interviews with fictional characters and organisations in a fictional region provide images of different aspects of NetForce Command and how they are interrelated: organisation, interaction and collaboration, self-synchronisation, orchestration, leadership, decision-making and information management.

4.1   Tour A: Emergent NetForce

Tour A 'Emergent NetForce' provides an impression of NetForce Command Archetype A, the most extreme implementation of NetForce Command, as the edges on e.g. empowerment of nodes, distribution of information and the absence of formal organisational structures are reached. Archetype A, as depicted in figure 33, is a NetForce Command implementation in which a NetForce emerges out of activities of different civilian and military nodes who are all committed to a high-level common objective in a certain complex, dynamic mission environment, for example reconstruction of an area after an earthquake, or restoring safety and security after a conflict, etc.
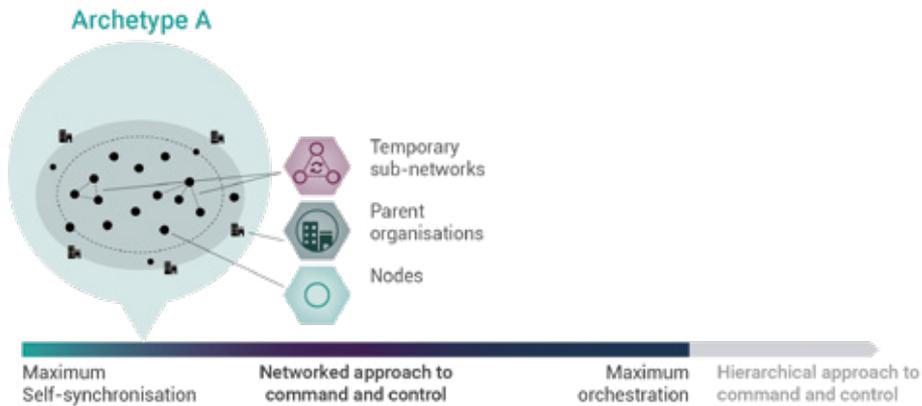
Figure 33 Illustration of NetForce archetype A

Military and civilian actors may contribute to a NetForce with one or more nodes and function as their parent organisation. It is also possible that a node functions without a parent organisation, for example volunteers with specific skills and idealistic motives like teachers or hackers. Furthermore, in the surroundings of the NetForce you may find actors that choose not to be part of the NetForce explicitly. These actors may be neutral, supportive or unsupportive to the intention or high-level objective(s) of the NetForce. In principle, the network has a fluid structure, which means that actors can decide at all times to leave the NetForce or to become part of it.

In archetype A the civilian and military nodes operate by self-synchronising their activities; they harmonise their activities and create unity of effort amongst each other. In general, the nodes may be influenced or consulted, but not commanded or controlled by any one of the other nodes. They may form temporary sub-networks in which two or more nodes collaborate and self-synchronise for a complex activity. In these sub-networks temporary hierarchical command structures are still possible at local level, for example to plan and execute a combat action.

Tour A 'Emergent NetForce' provides an impression of NetForce Command Archetype A from multiple perspectives: the perspective of a military node, the perspective of a civil-military node and the perspective of a parent organisation contributing to NetForce with one or more nodes. In the following sections you can read interviews with people representing these different perspectives.

A military node's perspective

Peter W. was member of a Special Forces unit of the RNLA Special Forces[30], that was deployed in the Termina region. This unit, consisting of eight pax, operated fairly autonomously. We spoke with Peter about his experiences.

Peter W.

Member of a Special Forces unit of the RNLA Special Forces

---

30. Peter W. is a fictional character and not actually a member of a Special Forces unit of the RNLA Special Forces.

What was the mandate and context of your deployment?
"The mandate of the NetForce that we were part of was to monitor and control the Brutopian infiltration in order to prevent Brutopian's growing assertiveness and to decrease its influence, especially in the Latverian city of Doomstadt and its surroundings. This included monitoring the potential influence of Brutopian information strategies on the ethnical Brutopian population in the Termina region. Our unit is specialised in counter-terrorism, direct action, special reconnaissance and surveillance operations, military support, and hostage rescue on land and sea. We specified our objective in NetForce as follows: control the unrest in the area, especially at the border between Latveria and Brutopia and make sure that all critical infrastructure is protected against possible threat. We had the freedom to specify our own objective based on a more general purpose for deployment in NetForce and to make our own decisions about which actions to take, which nodes to work with and which connections to establish."

> ### "We had the freedom to specify our own objective
> based on a more general purpose..."

With what other nodes did your unit interact and/or collaborate?
"Initially we had interaction with a Special Reconnaissance unit of the British Army that was carrying out surveillance missions throughout the city of Doomstadt and following and observing suspected Brutopian infiltrators. Also we interacted with a Swedish infantry platoon that was protecting critical infrastructure. We had to deconflict on the locations that we were operating in and we made arrangements to share relevant information on suspicious infiltrations and important locations of critical infrastructure.

About a month after our deployment, we were contacted by Mike from our Defence Operations Centre back in the Netherlands. They had received a question from a StratCom / Cyber unit to ask for support in countering the Brutopian information strategies. Mike told us about a sub-network that was being formed to work together on this objective and argued that our support could enhance the potential work of this sub-network. So, we joined this sub-network and I became the representative of our unit within this sub-network."

Can you describe the interaction and collaboration of your unit with others for me?
"The alignment with the Special Reconnaissance unit of the British Army and the Swedish infantry platoon was relatively basic. We agreed to contact each other on a daily basis via a secure voice and data communication channel. During these short conversations we spoke of our intentions for the following day, identified potential overlap and made appointments to deconflict where necessary, especially on the locations that we were operating in. Via this secure voice and data communication channel we also shared relevant information on suspicious activities and possible threats to critical infrastructure. This was done whenever relevant, so also in-between the daily 'meet-ups'. We all used our own local portable data devices to store the relevant information, so that we had the latest information available as much as possible, even in case of communication technology failures.

The collaboration in the sub-network was far more intense. The sub-network consisted of a RNLA Special Cyber Ops unit, the StratCom / Cyber unit, the German Cyber Defence Detachment 303, the Latverian Intelligence Agency, the Latverian Stratcom & Media Task Force and the Termina Centre for Media Excellence, that hosted the meetings. O, and I almost forgot, a YouTube-specialist also joined us. In the first few weeks, we met two or three times a week to come up with an activity plan to counter the Brutopian information strategies, that I already mentioned earlier. The objective was twofold. At the one hand, we wanted to disturb Brutopian information channels, and at the other hand we intended to perform an information campaign aimed at the ethnical Brutopian population in Latveria ourselves.

My Dutch colleague of the RNLA Special Cyber Ops unit proposed an approach to create this activity plan. Globally this approach consisted of identifying potential activities to reach our objective, prioritising them, assigning the activities to resources and determining when, and in some cases where, to carry out these activities. The vast majority of the representatives agreed on this approach and because of his expertise my Dutch colleague got roped into leading this process and keeping it on track. As I mentioned, it took us several meetings, divided over two or three weeks, to perform this process and come up with an initial activity plan. A digital platform was set-up to store, process and share all the relevant information that we encountered and created during this period and afterwards. The representative of the Termina Centre for Media Excellence facilitated this digital platform and kind of managed the information on it. Of course, when more information became available and when activities of our activity plan were executed and the results of it became manifest, we adjusted our activity plan on a regular basis. We met every two or three days to discuss the progress, skip some intended activities and identify and add some new activities. This way, our plan iteratively improved and emerged into a kind of strategy. This was on ongoing process.

> " A digital platform was set-up to store, process and share all the relevant information that we encountered and created during this period and afterwards."

One of the first actions of our Special Forces unit in the execution of the activity plan was to support a cyber action to attack a computer server of a Brutopian 'troll' organisation. This organisation operated just across the Brutopian border and was very active on Facebook and Twitter. We had to break in in the building that hosted this computer server, to allow the cyber specialists to get access and perform their digital activity. Of course, I can't go into too much detail on that, because then I would reveal our modus operandi.

During the course of the activity plan, new nodes began contributing to the sub-network, because they possessed capabilities that weren't available before and could therefore perform new activities that we identified. For instance, various hackers were added to the sub-network."

How do you reflect on working in this self-synchronising variant of NetForce?

"I think this self-synchronising way of working suited us, I mean our Special Forces unit, very well, because we were already used to work fairly autonomously with broad decision rights. So, interacting with other nodes and collaborating within the sub-network and improvising based on changed situations and circumstances worked very well. We really saw the first results of our efforts to de-escalate the, at that time, rising tensions in the part of Latveria near the Brutopian border. However, it's fair to say that without the interference of RNLA Defence Operations, perhaps we wouldn't have been part of the sub-network, or at least not from the beginning. It might have been that my faint acquaintance with the commander of the RNLA Special Cyber Ops unit could also have led to our involvement in the sub-network, but valuable time would have been lost by then.

What I didn't speak of before is that besides the sub-network I mentioned, several other sub-networks also had emerged after some time. Some of these other sub-networks were also aimed at countering the Brutopian information strategies. When we were aware of this, we decided to meet with one or more representatives of those sub-networks to see if we could align our efforts even more by creating a tactical design on information strategy while acting in the environment. Once again, I had the honour to be one of those representatives, as if I wasn't already busy enough. After, I think, two or three meetings we decided that an orchestrating element had to be formed out of the various organisations that were involved in the various sub-networks. I think, the fully self-synchronising period of our deployment in the Termina region ended right there, but it was, again in my opinion, a sensible decision."

A civil-military node's perspective

Interview with Joanna Fitzer, an employee of the Latverian Stratcom & Media Task Force,[31] that operates in the Termina region with special focus on the city of Doomstadt and surroundings. We spoke with Joanna about the interaction and collaboration with other nodes in the Termina region.

Joanna Fitzer

Employee of the Latverian Stratcom & Media Task Force

There were multiple nodes deployed in the same area all with more or less the same objective. When did you become aware of this and how were you able to synchronise different activities?

"At first, we had absolutely no clue who else was around. Our job was to inform the population in the city of Doomstadt and surroundings about the growing infiltration of Brutopian citizens. So we started to increase situational understanding and to develop all kinds of information activities to inform the local population. While doing so we accidently ran into a unit of the RNLA Special Forces, who were executing a special reconnaissance operation in the same village. We started talking to each other and found out that we were both contributing to NetForce. John, the commander of the Special Forces unit already spend some time in this area, so he had a much better understanding of the situation, which was very helpful for us in the beginning of our mission. As we shared the same interest we also decided to share information on a more regular base. First via e-mail and phone, later via a secure governmental platform that we could both use. John introduced us to his network of nodes. This network consisted of nodes with a focus on the Termina region. We shared information about intended activities with each other, using a communication platform. That helped a great deal to synchronise activities.

---

31. Joanna Fitzer is a fictional character, who works for the fictional organisation Latverian Stratcom & Media Task Force.

We had the unwritten rule that everyone would share their intentions, when someone noticed that there were overlapping intentions. Often these nodes formed a temporary sub-network to further align their activities or to work together. One day I noticed that in Doomstadt there was a need for enhanced situational awareness on the influence of Brutopian information strategies on the ethnical Brutopian population in the city of Doomstadt. This is something we as Latverian Stratcom & Media Task Force cannot deliver by ourselves. So, we asked John and also used the network to find other nodes who were willing to support us in our effort. We especially needed reconnaissance capacity. When we identified all relevant nodes, we contacted them directly. With most of them we formed a sub-network and together we could deliver specific information on the influence of Brutopian information strategies in the ethnical population in the city of Doomstadt and we could develop relevant information activities to counter that influence."

You describe a very positive story, but how exactly did you collaborate within the sub-network?
"Yes, my experience is a very positive one, sorry about that. Working in a sub-network is like forming a soccer team. You all share the same goal 'have fun, play fair and win some matches', but the way to get there might be different. Also, at first you don't know who is responsible for what. You do know for example who will be a good goal keeper and who is a good defender, but you don't know who will organise the monthly outing or drink, and who is responsible for laundering the shirts. But after the first couple of trainings things will get set, tasks and roles will be divided and the group will start rolling as a team. This is the same for working in a sub-network. When we formed the sub-network on the influence of Brutopian information strategies in the ethnical population in the city of Doomstadt, we only knew each other's capabilities and interests, but we did not know how we should organise the team so that we could develop tactical approaches or decide on timings and sequence of activities. Like in a soccer team, a natural leader emerged. In our case this was Lydia Brokoshak, from the local Doomstadt newspaper. This worked really well! Lydia was an enabling leader, if you know what I mean. She stimulated all initiatives and encouraged everyone to participate. When initiatives were contradicting each other, she mediated between the contradicting initiatives and everyone agreed with her interference. And then we had Peter from the Special Forces unit, he took care of timings and provided the sub-network with a working process. By doing so he actually made sure we got things done, instead of talking and philosophising too much. The final decision to actually do something together was made by Lydia and we all felt comfortable with it as she was trusted by all and had proven to be impartial."

" **Working in a sub-network is like forming a soccer team.** "

I can imagine that it took time to form a well-functioning sub-network, did all types of collaboration took this long?
"No. I have to explain that there were various types of support between nodes, from which forming a sub-network is the closest form of support. Nodes could also exchange capabilities to support each other. For example, one day we needed a statistical analyst to run some statistical analysis on our data, a capability we did not have because we hadn't foreseen so much data when we deployed. We asked around who could help us out, and within a day a UK Psyops-team responded. We could borrow their analyst for a couple of

days. This was really great! We were able to find a correlation between a behaviour of the ethnical Brutopian population and their susceptibility to misinformation. Of course the UK Psyops team could also use this insight in their own campaign, so it turned out to be a win-win. But it is not always successful and sometimes you end up with a no, as nobody is willing or capable to provide you with support. We noticed that we had been asking for support a couple of times, but rarely provided any support. After some time, this turned against us. So, it was a big relief that John, from the RNLA Special Forces, caught the rumour that we were being perceived as 'always asking but never delivering'. He told us immediately and we could change our behaviour."

Perspective of the parent organisation of a node

Interview with Mike T., Director of Defence Operations of the Netherlands Ministry of Defence.[32] We spoke with Mike to learn more about the role of Defence Operations as parent organisation of the Dutch nodes that contribute to NetForce.

Mike T.

Director of Defence Operations of the Netherlands Ministry of Defence

What is the role of Defence Operations during missions in which a NetForce consisting of diverse civilian and military nodes tries to decrease the tension in the Termina region near the border with Brutopia?

"Hmmm, that is a difficult question to answer. We were used to contributing units to for example a NATO mission. When our government decided to contribute to a NATO mission, we had an enabling role in deciding how and with which units we could contribute. Together with the operational command to which the units report to, we supported and facilitated aspects of the pre-deployment training. When the units were ready for deployment, they became part of the NATO mission and the NATO chain of command. In theory, our role was solely to support and to maintain the conditions for deployment, but in practice we commanded and controlled the units because we are used to doing that and because we needed to ensure that the contribution of the units stayed in line with the national political agreements and agreements with NATO. Thus, the political aspect of our role made it challenging to stick with solely supporting the units and required us to get information about the mission environment, the activities of the units and the interactions and collaborations they entered into. National caveats and political dynamics may hamper an enabling role of Defence Operations towards military nodes in NetForce.

"National caveats and political dynamics may hamper an enabling role of Defence Operations towards military nodes in NetForce."

In this mission in the Termina region, there is no NATO chain of command and there are no political agreements with NATO to reckon with.[33] The NetForce in this mission is a fluid coalition of diverse military and civilian nodes that share a common objective, in this case decreasing tensions within the Termina region near the border with Brutopia. One challenge for Defence Operations in an emergent NetForce (archetype A) is, even more

32. Mike T. is a fictional character and not the real Director of Defence Operations of the Netherlands Ministry of Defence.
33. In theory, NATO can be part of a NetForce as parent organisation of some military nodes or NATO can function as a NetForce, which is not the case in the context of this interview.

than when contributing to a NATO Mission, to take on an enabling role aimed at creating conditions under which nodes can operate in a self-synchronising manner to contribute to the overall objectives of the NetForce. Nodes need to have the freedom to bend their mission and their command and control when the complex, dynamic and networked environment requires so. So, as Defence Operations we need to prevent control of the nodes, because it will hamper them in self-synchronising their activities and in contributing to the overall objective of the NetForce. I think, after a while, we will become better and better to avoid this potential pitfall.

However, when our government decides to contribute to NetForce with one or more military nodes, it will do so in the national interest and it will come with national caveats and political dynamics. So, the challenge for Defence Operations is to prevent that political control gets the upper hand and will have a negative influence on the functioning of the nodes. It requires another, more mediating role of Defence Operations: providing relevant political information to the nodes and providing information about the nodes to the political level, the minister of Defence, thereby increasing the connection between the political level and the nodes and contributing to mutual understanding. This mediating role should be a part of the overall enabling role of Defence Operations."

How can Defence Operations support the nodes in NetForce?
"Besides connecting and improving the mutual understanding of the political level, the minister of Defence, and the nodes, we can support in numerous ways. We provide information of intelligence agencies and information on political developments to the nodes. We support the nodes with analyses with regard to mission environment, but of course we also support the nodes with creating solutions for the logistical and medical challenges they are confronted with. We also improve lines of communication and provide new clothes and equipment. And of course, we also arrange pre-deployment training and education. And if needed, we arrange training and education during deployment, for example when nodes need to deploy their capabilities differently. And...I would almost forget, we also enable the integration of new technologies in theatre, so that the nodes can work with state-of-the-art technology."

With whom do you collaborate?
"As Defence Operations, we function as parent organisation for our nodes in NetForce. We collaborate with other parent organisations to increase situational understanding of the mission environment, but we also collaborate on developing solutions for logistical and medical challenges. And we support each other with lines of communication and lines of transport into theatre. Furthermore, the collaboration and specific pre-deployment training and education is also growing, because our nodes often interact and collaborate with nodes of other parent organisations."

Does support of Defence Operations also relate to development of a strategy?
"No, it doesn't. it is not the role of a parent organisation to develop a grand strategy. We believe that our understanding of the mission environment will never be sufficient to develop a strategy. When we would develop a strategy, it will become obsolete the moment we finish it, because the environment changes too fast, is very complex and often unpredictable. However, a strategy could be developed and continuously adapted at local level. We do support the nodes in developing and adapting their strategy continuously, for example by providing information or by introducing new technology."

4.2   Tour B: Emergent Orchestrated NetForce

Tour B 'Emergent Orchestrated NetForce' provides an impression of NetForce Command Archetype B. Archetype B, as depicted in Figure 34, distinguishes itself from Archetype A by the arising need for orchestration of activities of the civilian and military nodes. From archetype B to the far right side of the scale orchestrating elements are formed to contribute to shared situational understanding and to provide harmonisation support for designing, planning, attuning and aligning of activities of civilian and military nodes in order to realise desired effects in the mission environment.

Orchestrating elements may emerge bottom-up (from what starts as a temporary sub-network) and will provide harmonisation support when there occurs a need within the NetForce, but orchestrating elements may also be designed by the parent organisations or the overarching organisations and provide harmonisation support and guidance from the start. Depending on the mission environment and the needs of the NetForce one or more orchestrating elements are formed. The orchestrating elements can dismantle themselves and/or change their function and purpose when the needs of the NetForce change. However, it is expected that in contrast with temporary sub-networks orchestrating elements will often be required for a longer period of time.
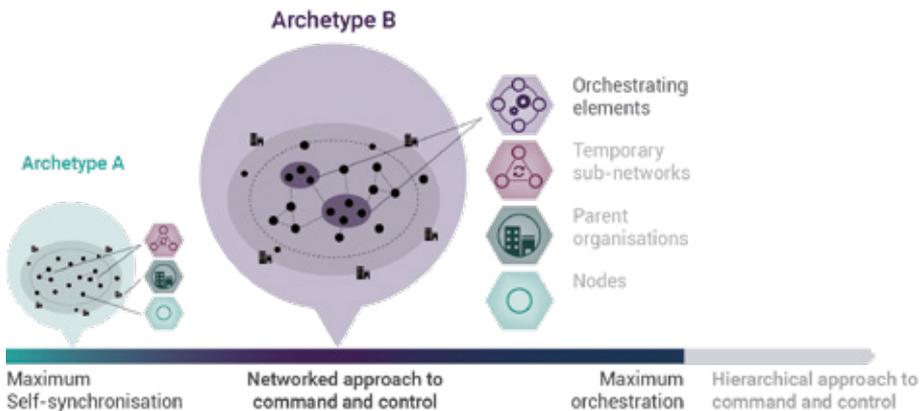
Figure 34 Illustration of NetForce archetype B

Tour B 'Emergent Orchestrated NetForce' provides an impression of NetForce Command Archetype B from multiple perspectives: the perspective of an orchestrating element, the perspective of a military node, and the perspective of a parent organisation contributing to NetForce with one or more nodes. In the following sections you can read interviews with people representing these different perspectives.

Orchestrating element's perspective

Interview with Chris de B., who was plans officer of a military Netherlands Information Operations unit that was deployed in the Termina region.[34] From this position, he represented the unit within an orchestrating element that was formed to create unity of effort with regard to the information campaign in the Termina region. We spoke with Chris about the functioning of that orchestrating element and its relation with other elements in NetForce.

Chris de B.

Plans officer of an Information Operations unit

What was the origin of the orchestrating element?
"Several temporary sub-networks that were aiming to counter the Brutopian information strategies on the ethnical Brutopian population in the Termina region, had become aware of each other. They decided to meet with one or more representatives of those sub-networks to see if they could align their efforts by creating a more overarching dynamic information campaign. After a few meetings they decided to initiate an orchestrating element to obtain this 'bigger picture' of their activities, as I would call it."

What were the main focus points of the orchestrating element and what was your role in the orchestrating element?
"As a logical consequence of the reason for initiating the orchestrating element, its main functions were developing an overall vision regarding the information campaign and the planning of different activities to execute that campaign. I was mainly involved in the development of the information campaign: integrating the different activities of the sub-networks into a narrative that created harmony between all the activities, communicating this narrative with nodes and sub-networks and supporting them in performing activities."

Which actors were involved in the formation and functioning of the orchestrating element?
"Because the orchestrating element fulfilled two functions (vision and planning) in developing the information campaign, its members came from a high diversity of involved temporary sub-networks. The members came from different backgrounds: strategic communication, (social) media, cyber, special operations, information technology, civil military cooperation. The members of the orchestrating element were a mix of both military and non-military public and private nodes."

How did the forming of the orchestrating element go?
"Initially we met two times a week, on Mondays and Thursdays. Work agreements were made upfront about discussion points and meeting agendas. Also agreements were made about how to share and store information. A digital platform was set-up. This was useful in the initial phase, in which we only saw each other two times a week. It allowed us to work on things and to communicate with each other outside the meetings. The initial phase mainly focused on setting up an organisation structure and tasks and responsibilities within this structure. According to the main purpose of the orchestrating element we defined several sub-projects: 1) developing an information campaign; 2) coordination within the orchestrating element; 3) improving shared situational awareness and understanding; and 4) providing harmonisation advice to the elements in NetForce. We were glad that we could use a part of the building of the Termina Centre for Media Excellence for our work."

---

34. Chris de B. is a fictional character, a fictional plans officer of a military unit for Information Operations.

How did the orchestrating element function in terms of internal 'command and control', if I may use these words?

"The work within the orchestrating element was more or less orchestrated. There was no formally appointed commander, but leadership emerged based on expertise and motivation. Leadership was often shared by more members depending on the situation and context. In that way we became more adaptive to handle the complex and unpredictable environment. Also decision-making took different forms. We did not use one fixed procedure. For the creation of a information campaign we used the method strategy knotworking. That is a dynamic, iterative and adaptive way of planning. It consists of six core questions with regard to collective purpose, context, the challenge, the starting point, a shared ambition and how to approach the future. The method of strategy knotworking leaves room for the members to consult the temporary sub-network they were part of and the parent organisation they represent. The method allows for adaptivity and improvisation when the context requires so."

"There was no formally appointed commander, but leadership emerged based on expertise and motivation. Leadership was often shared by more members depending on the situation and context."

With what other elements in NetForce did the orchestrating element communicate?

"Of course, especially in the beginning, the main communication took place with representatives of the sub-networks that initiated the formation of our orchestrating element. A number of representatives actually 'took a seat' in the orchestrating element and became a member. The representatives who did not became a member of the orchestrating element, acted as liaisons. In the first phase the orchestrating element was mainly focused on collecting information, ideas and objectives from the various temporary sub-networks in order to create 'a bigger picture' as soon as possible. Once that initial baseline was established, we were able to provide advice and suggestions on actions that we thought would be beneficial for the information campaign that we intended to develop. Needless to say that this process was not a 'one hit'-effort. Every day we received new information and results of actions, which led to adjusted visions and action plans, etc. Slowly, this led to development of an information campaign.

After a month or so, we became aware of another orchestrating element that had been formed to coordinate the activities of non-governmental organisations (NGO's) and other aid organisations. From that moment on, representatives of our orchestrating element met every two weeks with representatives of the other orchestrating element to discuss how the information campaign we were developing could support their efforts."

How much influence did your orchestrating element actually have on the other elements in NetForce?

"As I said, initially we were mainly in contact with the liaisons of the sub-networks that had initiated our orchestrating element. These liaisons trusted the members of the orchestrating element and because the sub-networks had expressed their need for some form of harmonisation support, they were inclined to 'listen' to our advice and suggestions. However, they were always critical and we had to prove ourselves regularly to maintain a sufficient level of trust in the work of our orchestrating element. When I say 'prove ourselves', I mean that we had to come up with good ideas, advise and suggestions. Overall, I think we managed to do so and over time we were even able to increase our area of influence to other nodes and sub-networks that became more open to our input and, consequently, provided us with additional information, as kind of compensation. Our ideas and suggestions also included adjustments in the composition of sub-networks, like adding new nodes to existing sub-networks, or even forming new ones and dissolving sub-networks that were, in our humble opinion, obsolete. When the parent organisations of the members in the orchestrating element saw that we were able to create, maintain, and sometimes even augment our area of influence, they were in some cases prepared to relax their guidelines and urge of control, which is something we can be very proud of, I think."

How do you reflect on working in the orchestrating element?

"As you probably will have noticed, I'm quite enthusiastic when I look back on my time as member of the orchestrating element. It is both stressing and exciting when you want to contribute to the work of temporary sub-networks and nodes without having a formal command relationship as we were used to in the past. Although there was some initial trust that had initiated our orchestrating element, there was not much time to enjoy this situation. We had to 'deliver' as fast as possible to prove our added value, and when we did, we were also able to help other elements. I think this is a sound development. Of course, in intense and time critical situations, a more strict form of command may still be valuable, but in general, I think, it enhances the overall performance and mission success, when influence is based on providing the right information to the elements you want to support. In that sense, orchestration really is a 'survival of the fittest'."

> " it enhances the overall performance and mission success, when influence is based on providing the right information to the elements you want to support. In that sense, orchestration really is a 'survival of the fittest'."

A node's perspective

A quick reaction of Peter W. confirms the story of Chris. "To be honest, although we had contributed to the creation of the orchestrating element, I was a bit skeptical about it. I think, this is due to the fact that within our unit, we are used to work fairly autonomously with broad decision rights. So, we started with a bit of a 'wait and see'-mentality. But, quite soon, we noticed that the orchestrating element helped us, by providing better shared situational understanding, and after some time, they also gave us suggestions about actions to perform. For instance, they pointed us at new locations where important hardware for the Brutopian information activities was stored. This was an important piece of our information campaign puzzle, that we wouldn't have been able to figure out ourselves or in the initial sub-network we are part of. I think it is in the interest of all participants of a NetForce to contribute to the overall objective as much as possible, and this specific orchestrating element helped us in doing that."

Perspective of the parent organisation

Interview with Elizabeth Thatcher, who is the co-director of StrategicNarrative.inc, a consulting firm that helps to develop strategic narratives, define communication strategies and strengthen connections within interorganisational networks.[35] Elizabeth herself took part in the orchestrating element formed to provide harmonisation support with regard to the information campaign in the Termina region. We spoke with Elizabeth about the contribution of her firm to the orchestrating element.

Elizabeth Thatcher
Co-director of
StrategicNarrative.inc

Why did you contribute to the orchestrating element for the Information Campaign in the Termina region?

"Initially, we contributed to a strategic coalition, but we noticed that in complex, dynamic and networked mission environments, information campaigns need to emerge in the field. We believed that we could contribute more effectively in an orchestrating element. When we were told that several temporary sub-networks that performed diverse information activities wanted to initiate an orchestrating element to harmonise all activities, we offered our services. The core business of our firm is to develop strategic narratives, which is very useful for harmonising different activities and for creating a more powerful influence."

How did you contribute to the orchestrating element?

"We contributed by supporting the development of a strategic narrative that glues all the information activities together into a coherent story that the local population could understand and support. So, as member of the orchestrating element, we mainly supported the project 'Development of Information Campaign'. We suggested to use the method strategy knotworking, including liberating structures, for the continuous development and adaptation of the information campaign. We also provided advice on communication activities that could support the Information Campaign."

---

35. Elizabeth Thatcher is a fictional character, who is the co-director of the fictional organisation StrategicNarrative.inc.

How did you experience the collaboration within the orchestrating element?

"The collaboration within the orchestrating element was very motivating and inspiring. The orchestrating element consisted of very different members that all contributed from their own perspectives and disciplines. It was inspiring to see how all these different disciplines came together into the development of an information campaign. Of course, the collaboration was not without heavy debates and discussions, but that is not strange considering the different backgrounds and the parent organisations that were represented. The debates and discussions are an essential part of the process of developing something that actually works in a complex, dynamic mission environment. Fortunately, most parent organisations that were represented in the orchestrating element, have chosen an enabling role towards the orchestrating element, which worked very well. The ones that did not, retracted their representative because they could or would not compromise and put own interests above the interests of the orchestrating element."

Did you have contact with the temporary sub-networks and nodes that benefitted from the orchestrating element?

"I did occasionally, but only when requested. Considering the nature of our contribution, it was not necessary for me to focus on the connections with the nodes and temporary sub-networks. The strategic narrative was developed with their input and the information campaign emerged out of their activities. Most of the interactions with the temporary sub-networks and nodes was done via the representatives of the sub-networks that initiated the orchestrating element and became a member. They already knew all the temporary sub-networks and nodes. So, I could focus on my expertise and on using it to facilitate the work of the orchestrating element."

4.3   Tour C: Strategic Orchestrated NetForce

Tour C 'Strategic Orchestrated NetForce' provides an impression of NetForce Command Archetype C. Archetype C, as depicted in figure 35, is a NetForce variant that differs from archetype A and B in the sense that the NetForce is supported and influenced by a coalition on political strategic level, a strategic coalition. A strategic coalition for specific mission environments consists of political strategic representatives of different actors, JIMP organisations, that also contribute to the NetForce with capabilities, and can also be formed by overarching organisations like UN, EU or NATO. From archetype C to the far right side of the scale a strategic coalition can have orchestrating influence on the nodes, temporary sub-networks and orchestrating elements in a NetForce in different ways: providing support, information and state-of-the-arte technology, networking with other actors, forming of an orchestrating element, influencing via the orchestrating elements, influencing the nodes and temporary sub-networks directly etc. Because of the political strategic level and the position of a strategic coalition, it is likely that it will exert influence directly and/or indirectly via the orchestrating elements.
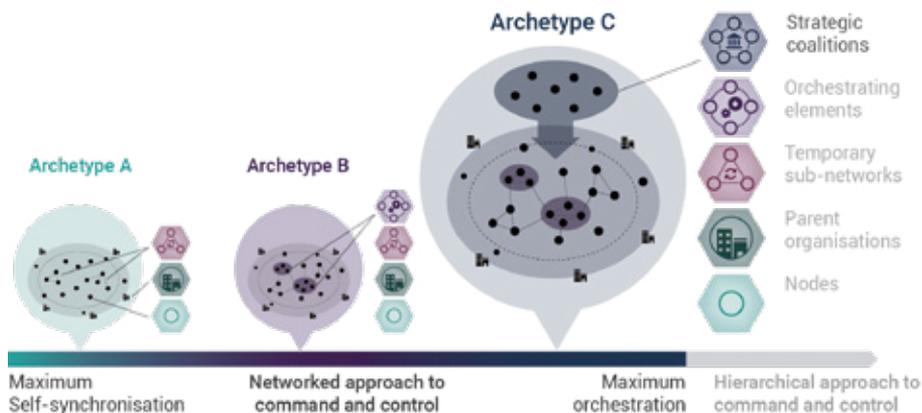
Figure 35 Illustration of NetForce archetype C

Tour C 'Strategic Orchestrated NetForce' provides an impression of NetForce Command Archetype C from multiple perspectives: the perspective of a strategic coalition, the perspective of an orchestrating element, the perspective of a military node, and the perspective of a parent organisation contributing to NetForce with one or more nodes. In the following sections you can read interviews with people representing these different perspectives.

Strategic coalition's perspective

Interview with Hannah M, who is a member of the strategic coalition for cyber security in the Termina region that was formed last year to harmonise efforts of different European governments and organisations that work in the field of cyber security. Hannah is working for the Netherlands Ministry of Defence and has years of experience in strategic design and planning of military operations.[36] We spoke with Hannah to learn more about the role of a strategic coalition in NetForce.

Hannah M.

Member of the strategic coalition for cyber security

Can you explain what a strategic coalition does?

"Yes, ... a strategic coalition is often a coalition on political strategic level. In our case, the coalition consists of strategic representatives of five defence departments of European countries and six cyber security organisations. In general all strategic coalitions want to have influence on the efforts of nodes, temporary sub-networks and orchestrating elements in NetForce. The role of our strategic cyber security coalition is to provide nodes, temporary sub-networks and orchestrating elements with information on new technological developments and essential state-of-the-art technology to execute cyber security activities. Because the field of cyber security is changing and developing very fast, it is not only important to collaborate in the field, but also on strategic level. On strategic level we can create insight in the latest developments in cyber security and we can develop innovative ways to tackle the challenges that cyber-attacks present to nodes and temporary sub-networks in NetForce. Furthermore, we can support the collaboration between different defence departments and companies that develop technology to improve cyber security and to prevent cyber-attacks. And we can even

---

36. Hannah M. is a fictional character who contributes to the fictional strategic coalition on cyber security, but is not actually working for the Netherlands Ministry of Defence.

support with the finance of new technologies. In a nutshell, our strategic coalition is aimed at supporting the nodes, temporary sub-networks and orchestrating elements in NetForce as well as we can with information, technology, ideas for innovative cyber security operations and finance of these operations."

How do the members of a strategic coalition collaborate?
"Collaboration is something that arises, not something that is there from the start. When it is clear which actors contribute to the strategic coalition, the interaction between the members of the strategic coalition is started. In our case, we discussed the function and purpose of the strategic coalition and the organisation of the strategic coalition, including role division, ways of communicating, information sharing and decision-making. They kind of emerged from the discussions. To be honest, the first couple of face-to-face meetings were focused on shaping the functioning of a strategic coalition. Many things were discussed, conflicts were solved and solutions emerged. The discussions felt like a precondition for actually working as a strategic coalition.

When the collaboration within a strategic coalition is kind of settled, a strategic coalition begins to function. To be able to contribute effectively to the complex and dynamic mission environment we meet regularly and then have the possibility to share information and discuss developments and issues face-to-face. In between the meetings, we share information and knowledge via e-mail, chat, and phone. In a later stage one of the members started to manage all the information that went round."

Who is in charge in a strategic coalition?
"It may sound strange, but no one is in charge. In our strategic coalition all members, representatives of different organisations, are equal contributors, although they may contribute different things: innovative ideas, insight in newest technologies, development of new technologies, information and situational understanding of the mission environment, and/or finance for innovation or to support cyber security activities and operations. Although formally no one is in charge, often one member is asked to take on the role of chairman during the meetings. Or a member takes that role naturally, which is fine as long as other members do not object. Often, there is also a member that is asked to perform the role of secretary during the meetings. This may be a different member of the strategic coalition for each meeting. In time, the role division between members of the strategic coalition often becomes clearer based on expertise, personal interests and personalities."

If no one is in charge, how does a strategic coalition make decisions?
"We make decisions based on consensus or the vote of the majority. Most decisions are preceded by a period of negotiations between the different members and their parent organisations. The negotiations are influenced by the developments in the mission environment, the resources, potentials and interests of the parent organisation of each member, and the surrounding network. Often members are open and explicit about their stances and implicit about their underlying interests. During the negotiations options can be expanded, modified, or restricted. However, most negotiations are initiated to realise a mutual gain."

What to do when negotiations go nowhere and lead to conflict?

"That does not happen very often, but when they do, a process of reconciliation is often started implicitly or explicitly by one or more members in the strategic coalition. When the issue or dispute can be solved within the strategic coalition, that is preferred. However, when negotiations go nowhere, this will often have to do with the underlying interests of the parent organisations. In those cases, parent organisations need to discuss their issues in dyadic talks and see whether they can come to an understanding or agreement. When they do, this will have a positive effect on the collaboration in a strategic coalition. When they don't, it could mean that one or both members will leave the strategic coalition and search for collaborations elsewhere."

Does a strategic coalition also develops a strategy and a roadmap?

"Hmmm...I am inclined to say that a strategic coalition should not develop a strategy, design or roadmap, but in practice, there are strategic coalitions that develop them. Often, these strategic coalitions or the parent organisations represented in these coalitions want to influence the activities of nodes, temporary sub-networks and orchestrating elements, sometimes for genuine purposes, for example to contribute to unity of effort, and sometimes to make more profits by increasing the use of their own capabilities.

I think strategic coalitions can contribute to improving strategies that are developed in the field, which is in line with the role of strategic coalitions that I explained earlier. I believe that in complex, dynamic environments, strategies emerge in the field, where nodes and temporary sub-networks interact with their environment and continuously act and sense what is happening. I know that in the past, we improved and enhanced some of the cyber security strategies that were initiated in the field."

How much influence does a strategic coalition have on the nodes, temporary sub-networks and orchestrating elements in NetForce?

"To my opinion, a strategic coalition should have a positive and supporting influence on the nodes, temporary sub-networks and orchestrating elements in NetForce. As said earlier, the strategic coalition for cyber security is aimed at supporting the nodes, temporary sub-networks and orchestrating elements in NetForce with information, technology, ideas for innovative cyber security operations and the finance of these operations. Supporting does not mean commanding and controlling the elements in NetForce. I think it would even be counterproductive for the nodes, temporary sub-networks and orchestrating elements, if we would try to command and control them. First of all, we do not have the situational understanding, they have. Second, we focus on cyber security, while most of the nodes, temporary sub-networks and orchestrating elements are confronted with many more challenges. If we would try to develop a plan for cyber security, we will have no idea whether or not it will conflict with activities or operations they execute in the physical or human environment. So, we can best support them by providing insight in cyber security development, making new technology accessible for them and by suggesting new ways of conducting cyber security activities and operations. Most of the time, we provide our insights, ideas, support and knowledge to the orchestrating elements, who know far better than us how to integrate these with other activities in the mission environment. Therefore, we mainly collaborate with orchestrating elements and try to make their lives a little bit easier. On specific topics, for example implementing a specific cyber security technology or conducting a specific cyber security operation, we may collaborate temporarily with nodes or temporary sub-networks that are involved."

How do you prevent having too much influence as a strategic coalition?

"That is not easy. And requires self-reflection. The members of a strategic coalition need to be aware of their supporting role. That role will be challenged continuously by internal as well as external forces. For example, internally there are always dominant personalities that want to put their mark on things and want to increase their power and influence. When these internal forces become counterproductive, other members of the strategic coalition will try to bend that influence into more positive directions. Externally, the influence of member's parent organisations may be challenging, especially when the ambition and interests of the parent organisation conflicts with the ambition and interests of the strategic coalition. Most parent organisations will strive for efficient deployment of their capabilities. However, when the deployment of those capabilities is not in line with what is required in a mission environment and a strategic coalition supports a change in deployment, tension arises. In those cases, enabling leadership is needed to switch between the needs of the parent organisations involved and the needs of the complex, dynamic environment. When one or more members are capable of enabling leadership, they will be able to perform ambidextrous leadership and come up with a balanced "both robust and agile approach" that is efficient for the member's parent organisations and effective for the nodes, temporary sub-networks and orchestrating element in NetForce."

> " When one or more members are capable of enabling leadership, they will be able to perform ambidextrous leadership and come up with a balanced "both robust and agile approach" that is efficient for the member's parent organisations and effective for the nodes, temporary sub-networks and orchestrating element in NetForce."

Earlier you said no one is in charge of a strategic coalition. How does ambidextrous leadership relate to that?

"To my opinion, leadership is not equal to control. In a strategic coalition, leadership emerges in the group dynamic process of social interaction between the members. Leadership will in most cases be manifested collectively based on specific expertise, knowledge or influence, but not on status or formal positions. Leadership functions may be distributed between different members or shared with all members in the strategic coalition. However, when all members of the strategic coalition agree, it is also possible to appoint a single leader."

Orchestrating element's perspective

Interview with Felipe H., who is a member of the orchestrating element focused on harmonising all kinds of cyber security activities of different nodes in the Termina region. Felipe works for the Spanish Ministry of Defence as cyber security manager.[37] We spoke with Felipe about the functioning of the orchestration element and their relation with the strategic coalition on cyber security.

Felipe H.

Member of the orchestrating element focused on harmonising cyber security activities

---

37. Felipe H. is a fictional character who is a member of the fictional orchestrating element focused on harmonising all kinds of cyber security activities and does not really work for the Spanish Ministry of Defence.

What is the function and purpose of the orchestrating element?

"The function and purpose of our orchestrating element is to harmonise the cyber security activities as much as possible. Cyber is a hot issue here in the Termina region. Because Brutopia performs a lot of cyber-attacks on companies in the region, it has really become a threat for the communities in this region. More and more cyber security companies enter the area to support companies to defend themselves against these cyber-attacks. Consequently, Brutopia begins to shift the focus of the cyber-attacks to local and regional government infrastructures. To harmonise the activities of all these cyber security companies and to create some kind of unity of effort, some of the companies and military cyber security nodes suggested to form an orchestrating element to support the harmonisation of all these different cyber security activities, to prevent conflicting activities and to strengthen the power and influence of smart combinations of cyber security activities. So, the function and purpose is mainly focused on harmonising the cyber security activities."

> "The function and purpose of our orchestrating element is to harmonise the cyber security activities as much as possible."

With which elements in NetForce does the orchestrating element interact and collaborate?

"The orchestrating element interacts with all the nodes and temporary sub-networks that, to our knowledge, perform cyber security activities. We offer them the information we have. In other words, we provide them with our bigger picture of cyber security activities in the region. When new companies enter the area, they will soon learn about our existence and will find their way to us. However, the level of interaction with the nodes and temporary sub-networks differs. For example, there are cyber security nodes that perform covert cyber security activities. These nodes often tell us in which area or in which type of organisation they will execute their activities and request us to ask other cyber security nodes not to perform any activities there, because that could jeopardise the planned cyber security activities. There are also nodes and temporary sub-networks that work very closely with us. They provide us with a lot of information about their activities and request us to deconflict, coordinate and sometimes even integrate activities."

How would you describe the relation between the orchestrating element and the strategic coalition on cyber security?

"That relation is actually quite well. The strategic coalition is really supportive to our effort of harmonising the different cyber security activities. We use their information, their ideas on innovative cyber security operations, their options for financing cyber security activities, and the possibilities they create to use state-of-the-art cyber security technology. We provide information to the strategic coalition; information about developments in the mission environment, information about the cyber-attacks the Termina region is confronted with, and information about the nodes and temporary sub-networks in the region. The strategic coalition needs these types of information to continue their supporting role. On specific topics, for example implementing a specific cyber security technology or conducting a specific cyber security operation, the strategic coalition is working directly with the nodes or temporary sub-networks, which is a good thing, because otherwise we as orchestrating element would only function as a serving hatch."

What if the strategic coalition would try to direct the orchestrating element?
"That would really harm the relationship. They do not have the information or the situational understanding to know what needs to be done in the region. They focus on cyber security as we do, but contrary to them, we can coordinate and harmonise with other orchestrating elements that are related to activities in the physical and human environment. So, when they would try to direct the cyber security activities in the Termina region, we would seriously consider to look elsewhere for information, technology, finance and ideas. I really believe the strategic coalition is most valuable in a supporting role, providing insight in cyber security development, making new technology accessible and by suggesting new ways of conducting cyber security activities and operations."

A node's perspective

Interview with Jane Bennet, who is working for CyberAware.com, a company focused on increasing awareness on the effects of cyber-attacks and the importance of securing digital infrastructures.[38] We spoke with Jane about their relation with the orchestrating element and their relation with the strategic coalition on cyber security.

Jane Bennet
Working for CyberAware.com

What is the function and purpose of your unit?
"We try to increase cyber awareness amongst the population in the Termina region. Furthermore, we try to stimulate and convince the local population to secure all their digital infrastructures, because of the cyber-attacks from Brutopia."

With which elements in NetForce do you interact and collaborate?
"Sometimes we collaborate with other nodes, especially when we have the same target audience. When we want to develop leaflets, advertisements, video messages for social media, we often collaborate in a temporary sub-network that also includes nodes that provide graphic design and animations. Most of these interactions and collaborations are temporary. When the collaboration worked out, we often look for each other when another assignment comes by. We also collaborate with different orchestrating elements in the Termina region, most frequently with the orchestrating element on cyber security."

How would you describe the relation between your node and the orchestrating element?
"Oh, that relation is really good. They do not decide what we should or should not do, but they do try to harmonise our planned cyber security activities with the cyber activities of other nodes and temporary sub-networks. That sometimes means that we postpone our activities or that we adapt our activities a little and collaborate with other nodes. They also provide us with a lot information about the mission environment, the other cyber security nodes in the region and developments in the field of cyber security. Sometimes they offer suggestions for courses of action related to cyber activities, based on information that we do not have. In short, the orchestrating element is very helpful."

---

38. Jane Bennet is a fictional character who works for the fictional organisation CyberAware.com.

How would you describe the relation between your node and the strategic coalition on cyber security?

"We do not have much interaction with the strategic coalition. We know that they provide information, ideas, insights, new technology and finance for cyber security activities to the orchestrating element for cyber security activities, and that they are using all that to harmonise the many cyber security activities in the region as well as they can. I do remember that several members of the strategic coalition visited us a few years ago to help us with the implementation of a new cyber security technology. That was very helpful and supportive."

What if the strategic coalition would try to direct your node?

"We will not accept that, especially because our parent organisation is not part of the strategic coalition. I also think that our organisation would strongly object to such influence and that the director will start diplomatic talks with the parent organisations that are represented in the strategic coalition."

Perspective of the parent organisation

Interview with Jack Thornton, who is the director of CDI (Cyber Defence Incorporated), a company that develops advanced technological tools to secure infrastructures of interorganisational networks.[39] One of his experts contributes to the strategic coalition for cyber security in the Termina region that was formed last year to harmonise efforts of different European governments and organisations that work in the field of cyber security. We spoke with Jack about the contribution of his company to the strategic coalition for cyber security.

Jack Thornton
Director of CDI (Cyber Defence Incorporated)

Why does your company contribute to the strategic coalition for cyber security?

"To be honest, there are two reasons why one of our experts contributes to this strategic coalition. One reason is that we just want to sell our tools that secure infrastructures of interorganisational networks. After all, we are a company. The second reason is that we want to contribute to causes we support. And we believe that collaboration in the field of cyber security is essential to prevent cyber-attacks from Brutopia."

How does your company contribute to the strategic coalition?

"Well, we develop advanced technological tools to secure infrastructures of interorganisational networks. By contributing to the strategic coalition for cyber security, we created the possibility to bring state-of-the-art cyber defence technology to the field, to the nodes, temporary sub-networks and orchestrating elements that need it the most. Via the strategic coalition, we find our way to potential customers that need our cyber defence tools. Because they are confronted with new cyber threats every day, the strategic coalition also connects us to interorganisational networks where we can test new cyber defence tools and receive input for development of new tools."

---

39. Jack Thornton is a fictional character, who is the director of the fictional organisation Cyber Defence Incorporated.

How do you experience the collaboration within the strategic coalition?

"In general, I think the collaboration within the strategic coalition works very well for my company. Like I said, the connection to nodes, temporary sub-networks and orchestrating elements in the field is very useful for us. The expert that is contributing on behalf of my company is also very positive about the collaboration, because it contributes to the harmonisation and collaboration of different cyber security companies and several European governments. However, due to political reasons, the members that represent a European government unintentionally slow down the work of a strategic coalition. For example, the use of new cyber defence tools by governmental nodes often needs to be approved by the respective governments. Political approval often takes time and nodes may not have that time when confronted with cyber-attacks. So, sometimes, the collaboration within the strategic coalition is a bit frustrating."

Would your company continue its contribution when your cyber defence tools are not used?

"That depends.... When the support or advice of a strategic coalition to the elements in NetForce includes the use of our cyber defence tools, we will continue our contribution, even when the elements in NetForce disregard the cyber defence tools. In that case, it is interesting for us to understand why they are not interested. That could improve our tools in the long run.

When the strategic coalition does not incorporate our cyber defence tools in their support and advice to elements in NetForce, then it becomes less interesting for us to contribute to the strategic coalition. So when that happens, my expert will probably advise me to stop our contribution to the strategic coalition. After all, our contribution needs to be beneficial for the company as well."

4.4   Concluding remarks

This chapter offered three tours of potential implementations of NetForce Command: the emergent NetForce (archetype A), the emergent, orchestrated NetForce (archetype B) and the strategic, orchestrated NetForce (archetype C). Each tour consisted of interviews with potential future actors in very different roles. The interviews provide images of how self-synchronisation and orchestration may work in NetForce. The interviews also offer an picture of how interaction and collaboration are shaped and how leadership, decision-making and information management may emerge. And how these aspects of NetForce Command are interrelated.

Developing interviews from multiple perspectives like the ones in this chapter supports the development of NetForce Command. In a way the interviews are small thought experiments that allow us to evaluate different aspects of the NetForce Command concept. The small thought experiments in the form of interviews with future actors also lead to new ideas and improvements of the NetForce Command concept. If you are interested to learn more about (different aspects of) the NetForce Command concept, we refer to chapter 2 and 3. If you are eager to learn about a potential form of NetForce operations, we refer to chapter 5, that introduces hybrid swarming.
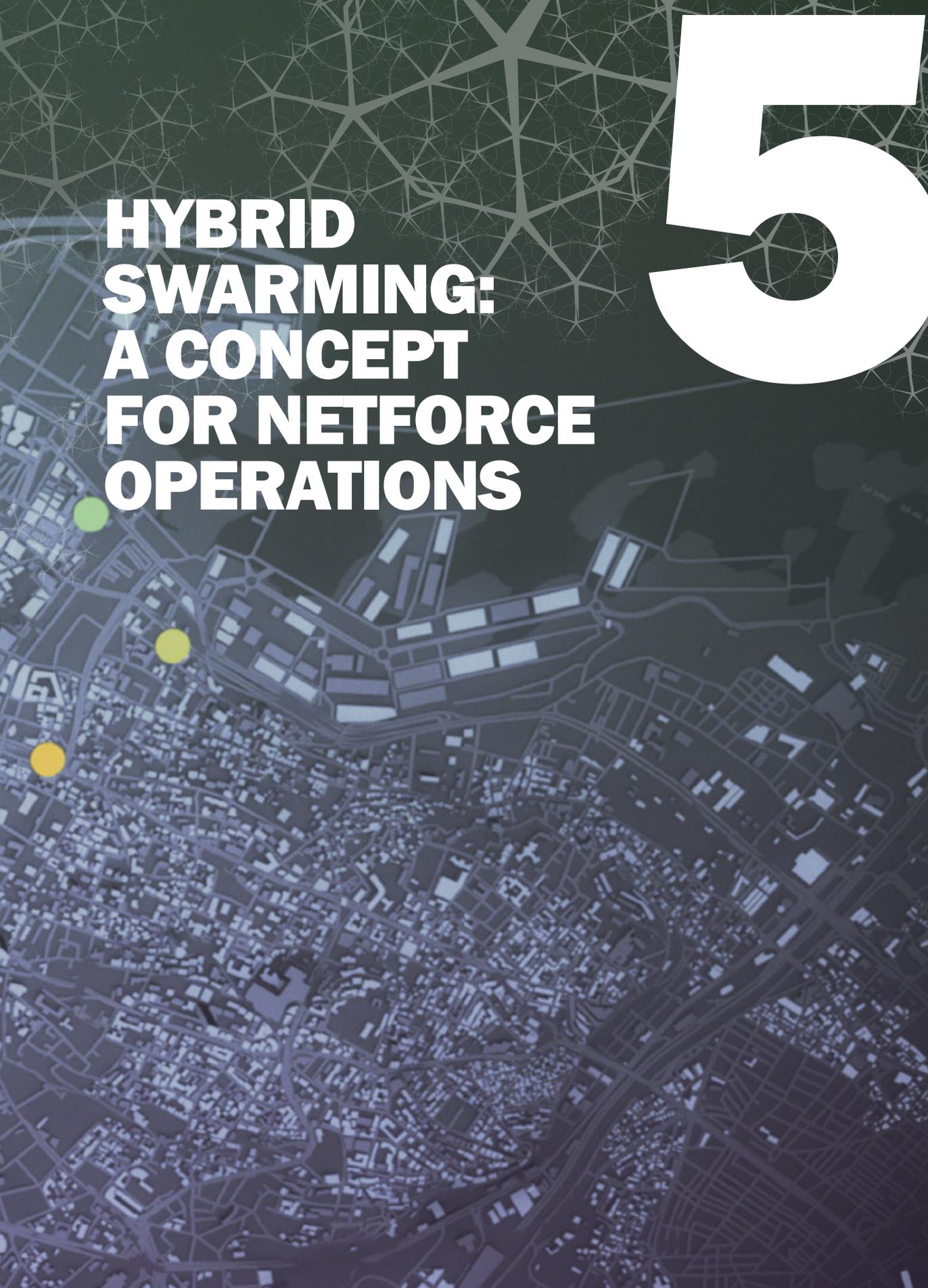
HYBRID SWARMING: A CONCEPT FOR NETFORCE OPERATIONS

5

5 HYBRID SWARMING: A CONCEPT FOR NETFORCE OPERATIONS

This chapter will introduce the concept of hybrid swarming, an approach to conducting future (NetForce) operations. The first section of this chapter will briefly recapture the nature and characteristics of the future mission environment and is followed by a description of the most important required abilities that will enable a force to conduct successful operations in such a mission environment. Subsequently, the concept of swarming will be explained as a prerequisite for the explanation of the concept of hybrid swarming. In the last sections we will elaborate on the idea that hybrid swarming is a promising approach to operations, which enables a force to be successful within the future mission environment.

5.1   Future mission environment

As explained in chapter 1, it is expected that the conduct of future missions will become increasingly challenging as a myriad of factors contribute to the increasing level of complexity, induced uncertainty and volatility of the mission environment. In modern military discourse, a mission environment is often conceptualised as a space which is composed of a physical, information and human environment, and framed by a political, legal and societal context. Within the Netherlands Armed Forces, these mission environments have been described in the 'three environments model' (Figure 36).
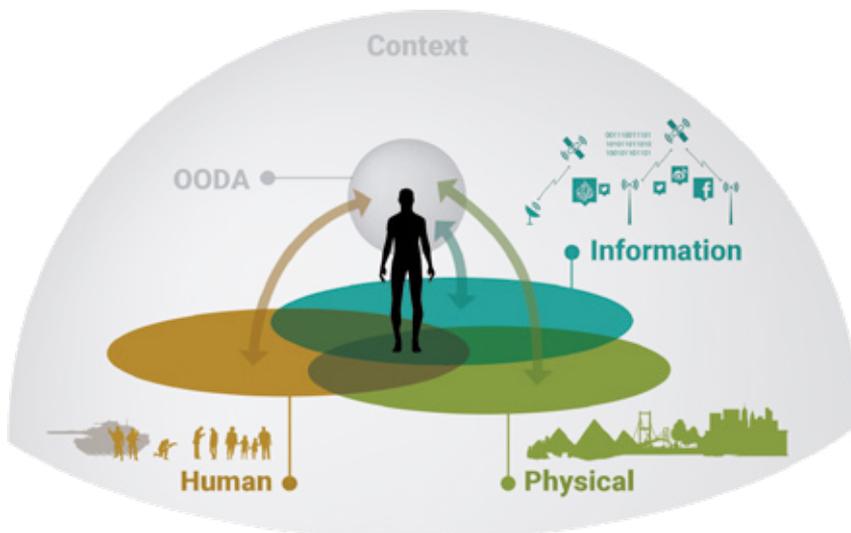
Figure 36 Three Environments Model (Land Warfare Centre, 2017)

As a short reminder, the *human environment* comprises the whole of individuals and organisations with their beliefs, values, interests, purposes and the interaction between them. The *information environment* includes all types of supply and transmission of information and data among which cyberspace and the electromagnetic spectrum. The *physical environment* comprises the environment where people live, including their supporting physical objects and infrastructure and where all physical activities take place. The physical environment remains important as opponents will use this environment that, combined with the other two environments, accommodates, amongst other things, influencing the local population and camouflage which are detrimental to western armies' traditional superiority in command and control, manoeuvre and Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR). As such, a mass of force(s) will still be required in order to control all aspects of the physical environment, especially in (dense) urban environments (Land Warfare Centre, 2017). These three environments often serve as a conceptual model to explain the recent change in military thinking which marks the human environment as 'the new centre of gravity'. Meaning that purposely (indirectly) influencing a target audience's perception and will, through activities in the physical and information environment becomes the new cornerstone for the conduct of future missions. This entails that a force's traditional focus on activities solely within the physical environment will not suffice when aiming to achieve the desired effects within the mission environment. This notion serves as the basis for the concept of hybrid swarming.

5.2   Required abilities for future operations

The mission environment's increased complex, uncertain, volatile and multi-dimensional nature puts both additional importance as well as extra stress on several abilities which are becoming increasingly important for the successful conduct of future operations and therefore future mission success. The most important required abilities are:

- **The ability to gain and maintain superior Situational Understanding (SU):** The mission environment is becoming increasingly complex, resulting in an increased level of uncertainty as cause-and-effect relations are difficult to point out and understand. Therefore, gaining a thorough understanding of the mission environment's underlying mechanics and dynamics becomes increasingly important to facilitate effective decision-making and in-situ (re)direction, coordination and (re)organisation of (to be) employed activities. Especially when adopting a command and control approach which is based on (a high degree of) self-synchronisation.
- **The ability to effectively influence the right target with the right activities, on time:** As cause-and-effect relations within the mission environment are becoming increasingly harder to specify and understand, it will become harder to detect, classify, localise, track and identify the right targets. In case the right targets are identified, it also becomes more difficult to determine the proper engagement method (the right actions) and subsequently evaluate their effect(s). Furthermore, the increased uncertainty decelerates the recurrence rate of the Observe, Orient, Decide and Action (OODA) loop. This decelerating effect is highly undesirable as the mission environment's increased volatility demands acceleration (at least to the level where it surpasses the opponent's OODA loop's recurrence rate) in order to be able to deliver the desired effects on time. The sum of these developments puts both additional importance and stress on a future force's ability to successfully determine and engage the right targets, on time.

- **The ability to be flexible and adaptive:** The complex, uncertain and volatile nature of the mission environment will manifest itself in fast and unpredictable changes. This means that a force will be required to be able to conduct a wide range of missions (flexibility) and to adapt to fast changing circumstances during deployment (adaptability). Of course, a sufficient level of situational understanding is required in order to effectively adjust to these fast and unpredictable changes within the mission environment, i.e. to effectively redirect, coordinate and reorganise ongoing activities.

It is deemed unlikely that the traditional approach to the conduct of operations will allow a future force to effectively cope with the mission environment's increased levels of complexity, uncertainty and volatility. The concept of hybrid swarming could provide an important additional approach to the conduct of operations that enables a force to effectively deal with the future mission environment's challenging nature. However, before elaborating on the concept of hybrid swarming and why it could meet future operational demands, it is important to explain the concept of swarming first.

5.3   The concept of swarming

Currently, swarming is a 'hot topic', especially within the area of unmanned (autonomous) systems and within the development of new operating concepts. Although swarming has recently received an increasing amount of attention, it is not a new concept. On the contrary, when looking at nature, swarming has been around for ages (e.g. flocks of birds or schools of fish). Regarding its military manifestations, military forces that employed swarming tactics can be traced back as far as Genghis Khan. To a certain degree, swarming tactics are still being applied by modern (western) military forces, for instance during ongoing operations in Afghanistan (Benda & Vink, 2017).

Figure 37 Swarm of birds (left photo); Mongolian warriors applying swarming tactics (right photo)

The question remains, what is exactly meant by swarming (tactics)? On a conceptual level, swarming can be decomposed into swarming behaviour and swarming intelligence. Concerning the first component, swarming can be described as a form of emergent behaviour amongst a large interacting set of nodes. Meaning that a swarm's behaviour depends on the relationship and interaction between the swarm's nodes, not on the swarm nodes' individual behaviour. Hence, swarming behaviour can only be effectively influenced and predicted by (a deep) understanding of the swarm's nodes and the relationship between them (Benda & Vink, 2017). In a military context, swarming behaviour (tactics) can be defined as a *"deliberately structured, coordinated strategic way to strike from all directions, by means of sustainable pulsing of force and/or fire, close in*

as well as from stand-off positions." (Arquilla & Ronfeldt, 2000). Swarming can be considered the most radical and sustainable form of non-linear tactics and operations (Edwards, 2004). Traditionally, the central idea behind the application of these swarming tactics was to defeat the opponent by swiftly and repetitively delivering a large number of precision strikes (in popular discourse often referred to as 'a death by a thousand cuts') instead of delivering one 'massive blow'. In other words, these tactics were aimed at gradually breaking an opponent's will to fight (causing moral collapse), not physical destruction.

Swarms can roughly be categorised in 'vapor swarms' and 'cloud swarms', depending on the level of density (i.e. the degree of dispersion between the swarm's nodes). A high degree of dispersion indicates a vapor swarm and a low degree of dispersion indicates a cloud swarm. When trying to meet a certain objective, swarms will generally use speed and mobility to disassemble and encircle the target through a double envelopment. Vapor swarms, on the other hand, will likely converge on a target from multiple directions, aiming to eventually form a ring-shaped annulus around the target (Ibid, 2004).

Cloud Swarm   Vapor Swarm
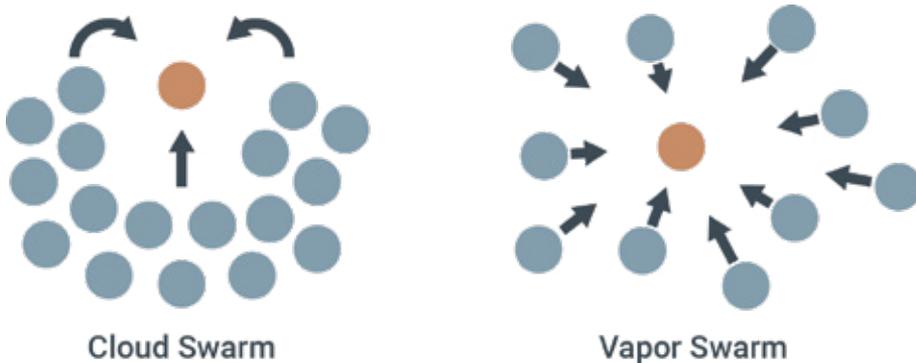
Figure 38 Cloud and vapor swarm behaviour

The swarm's nodes function as a sensor and effector as they are expected to function highly autonomously, making the swarm a potentially large and/or dense sensor and effector network, which enables it to quickly gain a high degree of situational understanding and subsequently conduct swift actions. Their behaviour is characterised by a high degree of speed, mobility and concealment (through a low signature), making them highly elusive. These characteristics generally entail that swarming nodes tend to be relatively small and light and therefore lack the ability to individually generate large volumes of engagement power (e.g. through fire power) and stopping power (e.g. through armour). A high level of elusiveness offers them protection and enables them to swiftly engage, disengage and re-engage a target (i.e. facilitates a high pulsating rate). This high pulsating rate enables swarms to deliver their relatively small amount of engagement power in a highly repetitive manner. Sufficient engagement power is generated through the combination of their large numbers and fast recurrence rate (Arquilla & Ronfeldt, 2000; Edwards, 2004).

Swarming intelligence, or in a military context: 'command and control within a swarm', is characterised by (a high level of) synchronisation. Briefly summarised, decision-making amongst swarm nodes is characterised by decentralised decision-making, synchronised by a common goal, intent and application of a common rule set. As a result, swarm nodes tend to be (highly) autonomous. This type of approach to command and control is deemed highly suitable for organisational structures that are required to function in complex and volatile circumstances (Benda et al, 2018). Note that the complexity of command and control within swarms grows with the number of nodes, their effector and sensor ranges, their degree of mobility, speed and/or concealment, and the volume of space in which they operate. For a more elaborate description regarding the mechanics and dynamics concerning self-synchronisation (and self-organisation), see section 3.1.

For successful swarming to emerge, various (pre)conditions need to be in place. The most crucial (pre)conditions being:

- **A superior Situational Understanding (SU):** having more information about the environment, including the opposing force, than the opposing force has about you. Having this superior information position enables simultaneity: self-synchronisation between the swarm's highly autonomous nodes. Furthermore, as a swarm's nodes tend to be light in order to be fast and highly mobile, they are heavily dependent on understanding the mission environment for their mobility and force protection. Having a superior information position supports swift and effective manoeuvre and protection (through a deep understanding of the mission environment's possibilities and probabilities for camouflage and coverage). Finally, especially regarding vapour swarms, having superior situational understanding is important in order to successfully disperse across the mission environment (while remaining a cohesive force) and avoid fratricide when engaging a target (Arquilla & Ronfeldt, 2000; Edwards, 2004).
- **Stand-off capabilities:** operations which are based on swarming principles generally take longer than more traditional (linear) type of operations due to their reliance on stand-off capabilities. As swarm nodes are mostly protected through their high degree of concealment, mobility and speed, and therefore tend to be light, they lack a high level of individual engagement and stopping power. Increased distance between a target (threat) and a swarm's node, while still being able to affect the target, increases a swarm nodes' degree of protection. Hence, possessing stand-off capabilities increases a relatively vulnerable swarm node's level of survivability, even against potentially 'larger' threats (Arquilla & Ronfeldt, 2000; Edwards, 2004).

A swarm's nodes and therefore the swarm as a whole are vulnerable to an opponent's efforts that aim to neutralise its (pre)conditions for success. Meaning that efforts which are aimed at degrading the swarm's mobility, speed, concealment, connectivity, superior situational understanding and employment of its stand-off capabilities could severely hamper the swarm's operational effectiveness. The theoretical concept of swarming is summarised in Figure 39, including its behavioural and intelligence properties and crucial (pre)conditions for success.

Theoretical Concept of Swarming

Behavioural properties
- Influencing the target from multiple directions by employing activities in a repetitive manner, synchronised in time and space, until the objective is reached
- Highly elusive through a high degree of mobility, speed and/or concealment

Intelligence (C2) properties
- Common goal, intent and rule-set
- High level of self-synchronisation and organization
- High level of autonomy

Crucial (pre)conditions
- Superior SU
- Stand-off capabilities

Figure 39 Theoretical Concept of Swarming (Benda & Vink, 2017)

Note that the military decision-making levels and the three environments (human, information and physical) are not included within the theoretical concept of swarming (in Figure 39). The concept of swarming is applicable at all military decision levels (Van Dalen, 2008) and within all three environments and therefore serves as the foundation of the hybrid swarming concept.

5.4   The concept of hybrid swarming

In the past military forces applied swarming (tactics) with the aim to change the physical environment. A military swarm's activities were heavily focussed on degrading an opponent's physical condition rather than on degrading its information position and/or ultimately its mental condition. Because the mission environment's human dimension is the new centre of gravity, changing a target audience's perception and will is now key in achieving a sustainable and desirable change within the mission environment. Although there is always the possibility in which this change is (or can be) achieved by military activities alone, it is more likely that the synchronised employment of a set of different activities based on the elements of national power, i.e. the DIMEFIL[40] elements, will induce that change and therefore bring about mission success. This is the main idea behind the concept of hybrid warfare (or the 'hybrid approach'). Although the concept of hybrid warfare is often mentioned within the context of geopolitics on the strategic level, its principles can also be applied to meet both operational and tactical objectives. When applying hybrid warfare principles to operational and tactical objectives, there is a connection with the concept of swarming. When examining the concept of hybrid warfare more closely, Benda and Vink (2017) identified more similarities between the concepts of hybrid warfare and swarming:

---

40. Diplomacy, Information, Military, Economic, Financial, Intelligence and Law Enforcement

- **The non-linear nature of both concepts:** the employment of a set of different DIMEFIL based activities can be interpreted as a non-linear approach to operations. Non-linearity, in a military sense, revolves around influencing a target from multiple directions. Each of the DIMEFIL elements can be interpreted as a 'direction'. Hence, by employing a set of activities which are based on the DIMEFIL elements, a force is able to influence a target from multiple 'directions'.
- **The elusive nature of both concepts:** due to hybrid warfare's complex nature and scale, it is a difficult approach to identify. Meaning that it is difficult to identify whether the various DIMEFIL based activities are purposefully employed and synchronised towards a specific objective, as part of a hybrid approach. As the conduct of hybrid warfare is hard to recognize, it is subsequently hard to effectively engage or employ counter measures on time, as the opponent is overwhelmed. The same rationale applies to swarming where initially concealed and subsequently elusive nodes employ activities which overwhelm the opponent, thereby hampering its ability to effectively engage or employ countermeasures on time.
- **The repetitive (pulsating) nature of both concepts:** a persistent and synchronised employment of DIMEFIL based activities is necessary to apply as much pressure as needed to meet the objective, i.e. achieve a sustainable and desired change in the mission environment. The same applies to swarming where activities are conducted in a pulsating manner and sustained over a sufficient period in order to wear down the opponent.

The similarities between both concepts all relate to their observable 'behaviour'. The main difference lays in the way the employed activities are directed, planned, coordinated and organised. The current command and control approach to hybrid warfare is considerably hierarchal in nature. This is not surprising considering that most modern militaries and governmental bodies are still based on hierarchical (i.e. conventional) principles and concepts. Although using a hybrid approach to operations does not exclude self-synchronisation as an approach of command and control, swarming explicitly demands such an approach in order to cope with the swarm's internal complexity and dynamics as well as to enable the swarm to effectively adapt to fast changing circumstances.

When combining the concepts of hybrid warfare and swarming, the concept of hybrid swarming emerges. Hybrid swarming revolves around the idea that a JIMP network adopts both the intelligence and behavioural properties of a swarm (see section 5.3) while applying an 'hybrid approach' in order to achieve a desired and sustainable change in the target audience behaviour. Or, more elaborately, hybrid swarming can be described as 'an elusive modus operandi, which aims to achieve (a) desirable and sustainable change(s) in the mission environment by affecting a target's physical condition as well as information position in order to gradually change a target audience's perception, will and therefore eventually its behaviour, over a sustained period of time. These changes are achieved through the repetitive, simultaneous and (highly) self-synchronised employment of a set of different DIMEFIL based activities, by a network of (highly) autonomous JIMP nodes' (Benda & Vink, 2017; Benda, Van Hekken & Ziekenoppasser, 2018).

The concept of hybrid swarming is captured in Figure 40, including its behavioural and intelligence properties and crucial (pre)conditions for success.

Figure 40 Theoretical Concept of Hybrid Swarming (Benda & Vink, 2017)

5.5 Hybrid swarming as a solution to future operational demands.

As mentioned in section 5.1, it is expected that the future mission environment will be characterised by a high degree of complexity, uncertainty and volatility. So what makes hybrid swarming a promising concept that enables a force to effectively operate in such a mission environment?

- **A hybrid swarm can swiftly gain and maintain superior situational understanding:** A hybrid swarm is composed of a network of highly autonomous JIMP[41] nodes which act as sensor and effector. As every JIMP node acts as sensor, a hybrid swarm potentially has the disposal over a large and diverse sensor network and information sources which yields a superior information position. As each JIMP node goes through a unique OODA loop, each of these JIMP nodes builds a unique information position. Assuming that the hybrid swarm is diverse and large enough to cover a broad range of the JIMP spectrum, a hybrid swarm has the potential to swiftly combine all of its JIMP nodes' information positions into a shared multi-dimensional information position concerning the state of the mission environment (for more information on Information Management in NetForce, see section 3.5). This shared multi-dimensional information position enables the hybrid swarm to gain and maintain a superior level of situational understanding. This superior level of situational understanding supports the swarm with specifying and understanding the cause-and-effect relationships, i.e. dealing with the mission environment's increased complexity and uncertainty. Note that gaining and maintaining superior situational understanding is also a crucial (pre)condition for effective swarming, as it supports simultaneity of effort, successful mobility, force protection by understanding the possibilities and probabilities for camouflage and coverage, successful dispersion, and avoiding fratricide.
- **A hybrid swarm can effectively influence the right target with the right activities, on time:** Based on the large and diverse sensor network and information sources of a hybrid swarm, shared multi-dimensional information position and subsequently superior level of situational understanding, a hybrid swarm is better able to detect, classify, localise, track and identify the right targets. When the right targets are identified, its

---

41. Joint, Interagency, Multinational and Public

shared multi-dimensional information position and subsequent superior level of situational understanding enables the hybrid swarm to determine the right engagement method more successfully. Due to the hybrid swarm's JIMP configuration and large size, it possesses a large as well as diverse effector network, which increases the chance that the right set of DIMEFIL based activities is available at the right place (target). Subsequently, a large and diverse sensor network and information sources enable the hybrid swarm to assess the achieved effects more effectively. Furthermore, the command and control approach of a hybrid swarm is based on self-synchronisation principles, which enables the hybrid swarm to make effective and timely decisions (i.e. to ensure that the activities are employed on time). The sum of these capabilities enables a hybrid swarm to effectively influence the right target with the right activities, on time. Thereby supporting the ability to deal with the future mission environment's increased levels of complexity, uncertainty and volatility.

- **A hybrid swarm can be both flexible and adaptive:** as a hybrid swarm's configuration consists of a large and diverse network of JIMP nodes, it can conduct a wide variety of missions (flexibility). The hybrid swarm's configuration is dynamic. Meaning that its nodes can join, participate and leave when required or desired based on the changed mission requirements, operational demands, expectations or interests. This dynamic nature allows a hybrid swarm to adjust to fast changing operational circumstances (adaptability). Because a hybrid swarm is composed of a large, diverse and dynamic (ad-hoc) JIMP network, it enables itself to be flexible and adaptable, thereby increasing its ability to deal with the future mission environment's increased levels of complexity, uncertainty and volatility.

5.6   Hybrid swarming and 'the new centre of gravity'

Current military thinking entails that influencing the human perception and will in order to achieve a desired change in behaviour, should be the ultimate objective when aiming to resolve a conflict as people initiate and resolve conflicts. Hence, the human environment is often referred to as 'the new centre of gravity'. Achieving such a behavioural change generally takes a long time as the human environment can only be influenced by indirect effects and will generally require a variety of activities which need to be applied over a sustained period. Hybrid swarming possesses two characteristics which, when combined, increase the chance of achieving such a behavioural change. The first characteristic being its configuration which is composed of a large and diverse set of networked JIMP nodes. As mentioned earlier, these nodes all act as both a sensor and effector, enabling the hybrid swarm to swiftly gain and maintain superior situational understanding and effectively influence the right target with the right set of DIMEFIL based activities, on time (see section 5.5). The combination of both abilities increases the hybrid swarm's chance of achieving the right effects in the physical and information environment, which yields the right indirect effects in the human environment. The second characteristic being the repetitive employment of its DIMEFIL based activities on a specific target (audience). This enables the hybrid swarm to influence a target over a sustained period (apply sustained pressure), thereby gradually altering the target audience's perception, will and eventually its behaviour. The combination of these characteristics enables the hybrid swarm to achieve desired behavioural change in the target audience during missions in a complex, uncertain and volatile environment, which is in line with the notion of the human environment as 'the new centre of gravity'.

Further Reading

Benda, R. & Vink, N. (2017). Towards Hybrid Swarming, an investigation into the Theoretical Concept of Swarming in both the Physical, Information and Human Landscape. *TNO report: TNO 2017 R11513.* Den Haag: TNO.

Benda, R., Hekken, M. van & Ziekenoppasser, L. (2018). V1604 C2 of Hybrid Swarming. TNO report: *TNO 2018 R11389.* Den Haag: TNO.

www.tno.nl/netforcecommand

IMPLICATIONS FOR THE ARMED FORCES

6

6   IMPLICATIONS FOR THE ARMED FORCES

In this book we describe NetForce Command (chapter 1) and introduce different implementations of NetForce Command, varying from maximum self-synchronisation to maximum orchestration. We also explain that implementations of NetForce Command differ depending on the composition, the organisation and structure, and the interaction in NetForce (chapter 2). We describe different NetForce Command concepts based on the social interaction between actors within NetForce (chapter 3). And we provide a tour of NetForce Command to make this alternative form of command and control more tangible (chapter 4). But what does NetForce Command mean for military units and the armed forces in general? Which challenges and opportunities do the implementation of NetForce Command pose to the armed forces? In this chapter we describe the implications of NetForce Command for military units and the armed forces along the DOTMLPFI[42] lines, which are essential factors for developing and implementing NetForce Command as capability. We describe the implications for training and education last, because all other implications require additional training and education. We are aware that we will not be able to provide a complete overview of all implications, because the development of the NetForce Command concept will continue and more implications will become clear in follow-up experiments and exercises with different aspects of NetForce Command.

Implementation of the NetForce Command concept widens the combat function *command* and gives substance to the new combat function *attune*.[43] However, NetForce Command will also affect four other combat functions: *shield, sense, affect*, and *sustain* (Land Warfare Centre, 2017; Van Dalen, 2017). Although these combat functions were not the focus of the NetForce Command research programme, we were able to organise three workshops in the field of logistics, communication and information systems (CIS) and manoeuvre to get a first impression of possible implications.[44] Outcomes of these three workshops are integrated in the description of the implications along the DOTMLPFI lines in the subsequent sections of this chapter.

---

42. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability.
43. This attune function was recently added in the Netherlands future land operating concept (Land Warfare Centre, 2017).
44. We chose these three fields in coordination with the Land Warfare Centre, because we believe that implementation of NetForce Command will pose many challenges to these three fields. We are aware that implementation of NetForce Command will also pose many challenges to other fields as well, but were not able to organise more workshops within the course of the research programme.

6.1 Doctrine

<div style="background: #3a2a56; color: white; padding: 10px;">

Doctrine: Expansion of command and control doctrine with NetForce Command

</div>

Contributing to a NetForce in a complex, dynamic mission environment does not necessarily mean that military nodes and their parent organisation(s), the armed forces, need to transform their hierarchical approach of command and control. Theoretically the armed forces and their military nodes can contribute to NetForce without changing their internal hierarchical approach of command and control. However, NetForce Command was specifically developed for complex, dynamic and networked mission environments in which a high operational tempo, agility and harmonisation of efforts are essential. Applying a hierarchical implementation of command and control in such an environment, makes it very challenging to increase operational tempo and to respond agilely to changing circumstances, as many military actions need to be approved in a chain of command, which requires time. Furthermore, interaction and collaboration (attuning) with civilian actors is not always supported by a hierarchical implementation of command and control by the armed forces, but it is supported by NetForce Command. It is even a principle of NetForce Command to focus on harmonisation of the efforts of military and civilian capabilities by stimulating and strengthening networked interaction and collaboration between all capabilities, thereby unleashing the power and influence of a NetForce. Therefore, it is preferred and probably even necessary that a military node that contributes to a NetForce applies NetForce Command, a networked approach to command and control, within their node. It is also preferred that the armed forces, as parent organisation, apply NetForce Command towards the military nodes that represent them in NetForce.[45]

When the armed forces want to be able to implement NetForce Command, this implies an expansion of current command and control doctrine with NetForce Command. The NetForce elements (see section 2.1), the archetypes (see section 2.2), the interactions in NetForce (see section 2.3) and the NetForce Command concept for self-synchronisation, orchestration, leadership, decision-making and information management (see chapter 3) provide input for expanding current command and control doctrines with doctrine for a networked approach of command and control. However, it should be noted that the NetForce Command archetypes represent just three possible implementations of NetForce Command and should therefore not be described as the norm in the development of new doctrine. Doctrine (especially at the level of how-to-think) should emphasise the broad range of possible networked and hierarchical implementations of command and control (see figure 41), their strengths and weaknesses and the importance of considering the context, the type of mission and the actors involved.

---

45. Note that NetForce Command is preferred for military nodes that represent the armed forces in a NetForce that operates in a complex, dynamic and networked environment. It is very well possible that at the same time the armed forces applies a hierarchical approach of command and control for internal processes or towards units that contribute or operate within an environment that needs a hierarchical approach of command and control.

Maximum
Self-synchronisation

Maximum
orchestration

Maximum
orchestration

Maximum hierarchical
command and control

Figure 41: Different implementations of command and control on a scale from maximum self-synchronisation to maximum hierarchical command and control

Expansion of current command and control doctrine especially concerns planning and decision-making in NetForce. To become effective in a complex, dynamic and networked environment, Tactical Designing is needed. Tactical Designing is an iterative process that supports decision-making in complex, dynamic and networked environments and provides an alternative for the often linear process of design, planning and execution. Tactical Designing seems a paradox, because design is often applied as a strategic planning process enabling decision-making on a strategic level and resulting in a masterplan, strategic plan or campaign that provides guidance to lower levels. However, when applied well, design begins and ends with clear iterations of a strategy and never results in a strategy that exactly describes how to achieve objectives from start to finish. Tactical Designing means that strategies are emerging iteratively in the field. Because full situational understanding is almost unattainable and always temporary, activities need to be planned and executed based on a general purpose. A more thorough understanding of the environment is gained incrementally by acting in that environment in line with that general purpose and idea, by monitoring changes in the environment, which may or may not be caused by one's own activities, by analysing and integrating the perceived changes and by adapting tactics or strategies accordingly. In other words, planning and decision-making in NetForce concerns a continuous process of doing, probing, learning and adapting in a complex, dynamic and networked mission environment. This process can be supported by a method that supports a dynamic, iterative and adaptive way of planning and decision-making: Strategy Knotworking.

Expansion of current command and control doctrine also concerns a shift from order to mandate. Military nodes need autonomy to cope with the complex, dynamic and networked environment through Tactical Designing, and to be able to interact and collaborate with other nodes in NetForce. Therefore, military nodes in a NetForce cannot operate effectively on an operations order; they require a mandate that provides direction and articulates the unacceptable conditions to address. A mandate may provide further direction by constraints and restraints, which may be adjusted over time. Intertwined with the mandate is a system for allocating decision rights. This system is flexible so it can be aligned with the chosen implementation of command and control. For instance, it could provide more autonomy when dispersed and (potentially) less when the operational reality calls for aggregated action and a (temporary) requirement for orchestration.

6.2   Organisation

Organisation: Not a transformation to a networked organisation, but a more enabling role of the armed forces.

Implementation of the NetForce Command concept does not mean that the armed forces as parent organisation need to transform their entire organisation from a hierarchically organised and structured organisation to a networked organisation, including a networked implementation of command and control. However, it is preferred that the armed forces, as parent organisation, are able to apply NetForce Command towards the military nodes that represent them in a NetForce.

Contributing to a NetForce with military nodes requires a more enabling role of the armed forces as parent organisation. The armed forces need to prevent control and micromanagement of their military nodes, because it will make them less adaptive and it will hamper them in (self-) synchronising activities and in contributing to the overall objective of the NetForce. Instead, they need to enable the nodes by providing information, analyses of the mission environment, solutions for logistical and medical challenges, communication and information systems, the implementation state-of-the-art technology et cetera. The armed forces also need to be able to organise internal networks of modules of military units and deploy them as modular military nodes in NetForce. However, the political aspect of the deployment of units makes it challenging to stick with solely enabling the nodes. This political aspect requires the armed forces to ensure that the contribution of their nodes is in line with national political guidance, intentions and caveats and with agreements with international organisations like NATO. In short, national caveats and political dynamics may hamper the enabling role of the armed forces towards military nodes in NetForce. To be able to operate effectively in a NetForce, a more mediating role of the armed forces, especially of Defence Operations, is required: translating the high(est) level of political information into ambition and intent in a language that is comprehensible for receiving nodes and providing information about the nodes to the political level, thereby increasing the connection between the political level and the nodes and contributing to mutual understanding.

6.3   Materiel

Materiel: Invest in robust, interoperable and secure information and communications networks

For the combat function command the implementation of NetForce Command does not require much new or additional materiel, except for information and communication technology. However, implications for materiel will become very clear with the impact of NetForce Command on the combat functions *sense, shield, affect*, and *sustain* (Land Warfare Centre, 2017), which was outside the scope of the research programme NetForce Command.

The performance of nodes in a complex and dynamic environment is heavily dependent on situational awareness and understanding and the ability to establish and maintain relationships with other nodes. In addition, the information position of nodes needs to be significantly extended and enhanced in order to enable them to make (self-synchronising) decisions. This transition requires the availability of a robust, interoperable and secure information and communications network in order to facilitate the production, exchange and dissemination of information between nodes, sub-networks, orchestrating elements, strategic coalitions and parent organisations. Because all these elements will be of a 'JIMP nature', the armed forces should, continue its efforts in improving joint and combined military communication and information exchange[46], and continue or even intensify its efforts in improving civil-military communication and information exchange.[47] However, a (JIMP) robust and secure information and communications network also requires a lot of attention for 'fallback' procedures, in case of malfunctioning of the technical network and for reasons of resilience.

Besides being able to communicate and exchange information between nodes, sub-networks, orchestrating elements, strategic coalitions and parent organisations, it is important to digitally support these elements in NetForce, and especially the nodes in understanding the complex mission environments and making adequate decisions. Next to descriptive digital support (presenting information in a clear and concise way), armed forces should also invest in diagnostic (deducting and explaining situations and information), predictive (suggesting how situations or own activities might develop) and prescriptive (suggesting or even taking decisions) digital support to be able to cope with the dynamics and uncertainty of complex mission environments.[48]

6.4   Leadership

Leadership: Invest in enabling leadership and collective leadership to make ambidextrous leadership a reality.

Implementation of the NetForce Command concept has implications for leadership concerning ambidextrous leadership, including enabling leadership, and collective leadership.

Ambidextrous leadership
Ambidextrous leadership (Rosing et al, 2011) is the type of leadership that seems to fit best as the basic leadership approach for nodes, parent organisations and NetForce collaborations to contribute in NetForce and to cope with the complex, dynamic multiparty mission environment. Ambidextrous leadership makes it possible to constantly adjust the balance of robust and agile approaches in order to deal with the tension between what the context requires and what most organisations and collaborations in NetForce are capable of doing. Future military leaders need to learn to apply a balanced robust and agile approach to challenges in the mission environment. Such a balanced approach is

---

46. The NL Defence program FOXTROT is to provide for a wireless IT infrastructure and command and control systems for military users during mobile operations.
47. The NATO Federated Mission Networking (FMN) program is is a governed conceptual framework consisting of people, processes and technology to plan, prepare, establish, use and terminate mission networks in support of federated operations.
48. These forms of digital support are the focus of the TNO research programme V1905 'C2-services for JIMP and flows'.

only possible when leaders are able to switch between closing leader behaviours to foster a robust approach (operational leadership) and opening leader behaviours to foster an agile approach (entrepreneurial leadership) (Rosing et al., 2011, Uhl-Bien & Arena, 2018). However, most leaders are inclined to favour either operational leadership or entrepreneurial leadership.

Ambidextrous leaders are capable of applying enabling leadership, which enables them to switch between and balance both operational and entrepreneurial leadership, despite their natural tendency to favour either operational or entrepreneurial leadership in all contexts. Enabling leadership sets the conditions for switching between operational and entrepreneurial leadership and for conducting the balancing act for a robust and agile approach. Enabling leadership is focused on creating, engaging and protecting the adaptive space and the adaptive process that supports and catalyses entrepreneurial leadership and that connects the results of entrepreneurial leadership to the formal systems, structures and processes governed by operational leadership. Military leaders need to master enabling leadership to be able to operate effectively in complex, dynamic environments. The armed forces should invest in enabling leadership to make ambidextrous leadership a reality.

Collective leadership

In NetForce collaborations like temporary sub-networks, orchestrating elements and strategic coalitions, leadership will often emerge from social interaction, which make collective forms of leadership necessary. A collective manifestation of leadership means that in a complex, dynamic environment more than one person can perform leadership. Collective leadership is defined as a social process in which leadership emerges from the social interaction of representatives of different nodes or parent organisations. Collective leadership can be distributed between different representatives or shared with more representatives. Following behaviours in combination with leading behaviours and context variables influence the form of collective leadership that will emerge. To be able to collaborate effectively in NetForce collaborations, military leaders need to understand that they will not necessarily have a leading role when collaborating with other actors. They need to be sensitive to the group dynamics and assess what kind of role is most suitable to take on. Furthermore, in many situations they will need to share their leading role with other leaders.

Collective ambidextrous leadership is not only possible in NetForce collaborations, but also in military nodes. It is even expected that emergent, collective ambidextrous leadership will make a military node in complex, dynamic and networked environments more effective. When the armed forces consider collective ambidextrous leadership as a possibility for military nodes in complex, dynamic and networked environments, it requires a change in mindset. Currently leadership is connected to the decision-making and command. However, unity of command in relation to decision-making and command & control can co-exist alongside collective leadership and functional decision-making based on expertise, knowledge, skills and personality. An example is the functioning of special staff officers from the engineers and artillery within a brigade staff.

Besides a change in mindset, military commanders need to have a certain openness towards subordinates who may acquire more leading influence based on their expertise, knowledge, and skills than a commander based on his function and position. It also requires self-awareness, the ability of military commanders to reflect both on themselves as an individual and on the status of their node (unit). They need to accept that in

complex, dynamic and networked environments they will no longer be able to have complete oversight on their own. They need their subordinates and other actors to understand the mission environment. Some will argue that in the armed forces military commanders on brigade level are supported by a staff for precisely that reason. However, in NetForce, military nodes will be smaller than a brigade and a military commander of a military node will not have the support of a staff at his disposal. Therefore, a military commander in NetForce needs to be open to leadership of others based on expertise, knowledge, and skills.

6.5   Personnel

Personnel: Invest in mindset and empowerment of military personnel

Implementation of the NetForce Command concept has different implications for personnel. These implications concern coping with hierarchical and networked implementations of command and control, manifestations of orchestration, empowerment, and a change in mindset.

Hierarchical and networked implementations of command and control

In order to implement the NetForce Command concept, military personnel need to be able **to operate in a broader range of command and control implementations** than for which they are currently trained and educated. They not only need to be able to operate in different implementations of a hierarchical approach, but also in different implementations of a networked approach (see figure 42).

Figure 42: Different implementations of command and control on a scale from maximum self-synchronisation to maximum hierarchical command and control

Depending on the context, the type of mission and actors involved, the most suitable implementation of command and control will be chosen. In practice, this could mean that personnel of military nodes need to be able to operate as autonomously as possible in one mission and to follow strict orders in the next. It could even mean that they should be able and flexible enough to change the implementation of command and control during a mission. However, we expect that in practice a switch will often not be that extreme, i.e. from self-synchronisation to a hierarchical implementation of command and control, but more subtle, for example from fully autonomous self-synchronisation to a form of orchestration. To be able to use and switch between different command and control implementations, personnel in military nodes should have the **ability to cope with a high level of uncertainty**. Nodes that are unable to deal with a high level of uncertainty will react too slowly and will not be effective in a highly complex and dynamic mission environment.

Manifestations of orchestration

To be able to operate in NetForce Command, personnel of military nodes need to be aware of the different potential forms of orchestration and when some level of orchestration is required and desired by the nodes. In NetForce Command, orchestration has the character of harmonisation support focused on creating unity of effort between nodes and temporary sub-networks. Harmonisation support is provided by orchestrating elements. Orchestrating elements cannot control the nodes, but can support and also influence them. An orchestrating element can contribute to the creation of shared situational awareness and support the harmonisation of designing, planning, attuning and aligning of activities of different nodes. The harmonisation support that is provided by an orchestrating element depends on the manifestation of an orchestrating element: its function and purpose, composition, organisation and structure, culture, and style of orchestration. Personnel of military nodes need to be aware of the different manifestations of orchestrating elements and the different forms of harmonisation support they can provide. Military nodes need to be able to collaborate as effectively as possible with all these different manifestations of orchestrating elements.

Empowerment

Implementing NetForce Command requires that military nodes are empowered by the armed forces and are able to function as empowered nodes. Empowerment means power to the edge of an organisation (to the nodes, temporary sub-networks and orchestrating elements), where the organisation interacts with the mission environment to have an impact or effect on that mission environment (Alberts & Hayes, 2003). Empowerment means coping with more autonomy and different and unprecedented new forms of mission command (from orchestration to maximum self-synchronisation) during deployment. Empowerment also means that personnel of military nodes are able to decide and act in line with the dynamic of the environment without going up the chain of command. Empowerment will require new and other abilities of military personnel related to:

- **Coping with different degrees of empowerment**, i.e. different degrees of freedom to decide and act, depending on the implementation of NetForce Command, the context, the type of mission, and the opponent(s) and actors involved;
- **Self assessment**: the ability that enables all military personnel and military nodes to gain insight in the status of own capabilities and the demands and capabilities of others. The ability to perform self-assessments is fundamental to prioritise and harmonise activities;
- **Coping with the complexity and dynamics of the mission environment**, which makes decision-making, leadership and command very challenging and sometimes even vulnerable;
- **Coping with the pressure** of making decisions with potentially far-reaching consequences based on limited situational understanding;
- …

In general, these abilities imply the demand of experienced and well trained and educated military personnel in NetForce. It is important to identify relevant competencies related to these abilities and to adapt selection, recruitment, training and education accordingly to acquire military personnel that are capable of operating in NetForce.

Change in mindset

Implementation of NetForce Command also requires a change in mindset of military personnel. To function as empowered nodes in a complex, dynamic and networked environment, military personnel need another mindset than a 'following and executing orders' mindset that suits a hierarchical approach of command and control. NetForce Command in a complex, dynamic mission environment requires a 'probe-sense-respond' mindset that can be characterised as exploring, creative, learning-by-doing and full of initiative. To unleash the power of a NetForce consisting of military and civilian nodes, and several temporary sub-networks, orchestrating elements and strategic coalitions, it is essential to work towards tangible objectives that are within reach and therefore attainable (as opposed to objectives in a distant, 'over the horizon' future). It is also essential to negotiate and to focus on reasonable trading opportunities for mutual gain. Especially in complex, dynamic and networked environments in which it is almost impossible to realise objectives and create effects solely. A mindset focused on harmonisation is essential because nodes do not have the mandate to control other nodes, and temporary sub-networks and orchestrating elements can only influence and not command and control the nodes. When all elements in NetForce focus on harmonisation in their decisions during interactions and collaborations, it becomes possible to create unity of effort and to perform a balanced and effective agile approach to cope with the complex and dynamic mission environment.

6.6   Facilities

> **Facilities: No direct implications**

Implementation of the NetForce Command concept does not have direct implications for facilities. However, there may be implications for the combat functions sense, shield, affect, and sustain (Land Warfare Centre, 2017), which were outside the scope of the research programme NetForce Command.[49]

6.7   Interoperability

> **Interoperability: Invest in Information Management and the social aspects of interaction and collaboration**

A NetForce receives its power and influence from its capabilities and its actions, and from the connections and interactions of the different military and civilian nodes in a network. In section 2.3 we introduced different types and levels of interaction varying from unawareness to collaboration or even integration. Interoperability is a prerequisite for interaction and collaboration of military personnel and military systems with the different (JIMP) elements in NetForce. Interoperability has many definitions which both refer to the ability of equipment, groups or organisations to operate in conjunction with each other and to the ability of computer systems or software to exchange and make use of

---

49. The combat function sense is the focus of the TNO research programme Sensing in a Networked Environment (SiaNE).

information. As a consequence interoperability may manifest itself at various 'levels': a technical level (communication protocols), a syntactic or data level (format of data), a semantic level (meaning of data), a procedural and a cultural level. In section 6.3 (Materiel), we already discussed aspects of the first three levels of interoperability and emphasised its 'JIMP nature'. In this section we focus on interoperability on the procedural and cultural level.

An important factor in interoperability is extending the information position of nodes and other NetForce elements through Information Management. At the moment, information management is still a relatively unexplored area for the armed forces. There is a focus on operational concepts and information and communication technology, but the connecting link (information management) has remained underexposed so far. An important first step for the armed forces is therefore to further develop IM capacity for the operational units. This IM-capacity will probably first have to learn to work according to the planned, coordinated approach of IM. At the same time, investments must also be made to increase awareness among operational users. They must realise that in fact every user (as information producer and information consumer) forms part of IM and has a responsibility to act by making information available and building and maintaining an information profile. A next step would be to educate and train own Information Managers in networking with other Information Managers (representing other communities), establishing procedural and/or technical interfaces between digital collaboration environments (or merging them).This will be crucial in a setting with various temporary sub-networks.

Furthermore, it is important to start experimenting with forms of digital support. This will help the transition to shift more IM functions to the user (information producer and information consumer). This will also help to change the role of the coordinating IM entity towards monitoring and adjusting the information sharing. A drawback of these recommended steps is that the introduction of more and more digital support, also means an increasing dependence on technology and thus a greater vulnerability. Resilience and 'fallback' options must not be added at a later stage as a complimentary package (or afterthought). Systems need to be resilient by design. Nevertheless, non-technical back-up plans still need to be developed and exercised. The first recommendation to set up an IM-capacity within the armed forces plays an important role in this regard.

Another aspect of interoperability concerns the interaction and collaboration within NetForce. The effectiveness of NetForce and NetForce Command is depended on the interaction and collaboration within NetForce. Military personnel need to be aware of the different types and levels of interaction they may have with different elements in NetForce: other nodes, temporary sub-networks, orchestrating elements and strategic coalitions. They also need to have an understanding of how interaction and collaboration is formed, developed and transformed. In other words, military personnel need to have an understanding of the four phases (positioning, shaping, executing and transforming) of interaction and collaboration, including how internal and external factors influence the course of these four phases. And especially the shaping of processes like management and control, decision-making, leadership and information sharing. To be able to create and leverage the potential power of interactions, especially collaboration and integration, military personnel need to be able to assess the advantages and disadvantages of interactions and collaborations in a temporary sub-network or orchestrating element. They need to be able to exploit the benefits and to minimise the risks of these interactions and collaborations. This is only possible when military personnel know that no interaction

is the same and interactions may change over time, depending on all kinds of internal and external factors. Finally, military personnel need to be aware that there may be huge differences between collaboration within their own military nodes and collaboration in temporary sub-networks and orchestrating elements with representatives of other nodes. All these implications of interaction and collaboration in complex, dynamic and networked mission environments require training and education.

6.8   Training and Education

> **Training and Education: NetForce Command requires experienced and well trained and educated military personnel with a flexible mindset.**

Implementation of the NetForce Command concept will have consequences for the *operational readiness process* of the armed forces. The operational readiness process[50] is a process focused on preparing capabilities (units/systems) to meet operational readiness standards. If a unit has achieved operational readiness status, it is able to perform the tasks for which the unit is organised or designed. The operational readiness process of a unit consists of three elements which are closely interrelated:

1. **Personnel readiness:** the extent to which military personnel are available, suitable and trained for conducting tasks and functions belonging to the military unit/ organisation;
2. **Materiel readiness:** the availability and maintenance of materiel required by a military unit/organisation to support its wartime activities or contingencies, disaster relief (flood, earthquake, etc.), or other emergencies;
3. **Training readiness:** the schedule and process of exercising and training in line with the tasks for a military unit/organisation. To be able to exercise accordingly, units require support of enablers: Combat Support (CS) and Combat Service Support (CSS) units.

Military personnel need to be trained and educated in operating in a broader range of command and control implementations: from maximum self-synchronisation to maximum hierarchical command and control. **Education on the broad range of command and control implementations**, especially about the differences between a networked and a hierarchical approach of command and control is required. Education should also include self-synchronisation and the different forms of orchestration in the networked as well as the hierarchical approach of command and control. Training of (personnel) of military nodes should be focused on the whole range of command and control implementations, from functioning as self-synchronising nodes to following orders in a chain of command. Training should also be focused on exercises with different forms of orchestration, varying from harmonisation support in NetForce Command (provided by different manifestations of orchestrating elements) to conducting sub-ordinates in hierarchical command and control. Lastly, training of military nodes should also explore the potential of switching between command and control implementations, including coping with the high level of uncertainty due to the complexity and dynamics of the mission environment.

---

50. In Dutch: gereedstellingsproces.

To be able to function in NetForce Command, personnel of military nodes need education on empowerment and on the importance of different degrees of empowerment in NetForce Command depending on the implementation of NetForce Command, the context, the type of mission, and the opponent(s) and actors involved. Training of military nodes should be focused on coping with different degrees of empowerment and on reflection related to own capabilities and the capabilities of other nodes in order to recognise the demands and needs of the mission environment. Training in self-assessment is fundamental for military nodes to be able to prioritise and harmonise activities with other nodes in NetForce. Implementation of NetForce Command may even require empowerment as default setting in training and education, because in the armed forces it currently is easier to downscale freedoms than to upscale to a level that most units are not yet accustomed to.

To be able to function as empowered nodes, military personnel need additional skills related to leadership and decision-making. Education and training of future military leaders should be complemented with theory and exercises on ambidextrous leadership, including the complexity leadership framework, and on creating a paradoxical mindset to be able to apply a robust as well as agile approach. Furthermore, future leaders need to learn to reflect on their own leadership style, their natural tendency for either operational or entrepreneurial leadership, and on their ability to switch and practice enabling leadership.

Most military leaders are not familiar with collective leadership. Therefore, future training and education of military leaders should also be complemented with theory and cases of collective leadership and followership, especially in settings of networked collaboration with other military and non-military actors. Military leaders need to learn to be open to leadership of others based on expertise, knowledge, and skills instead of formal position. Moreover, training and education of future leaders should be focused on the group dynamic process that comes with emergent networked collaboration with other actors.

Interaction and collaboration in NetForce requires a networked perspective: each element in NetForce is embedded in a set of interorganisational, technical and social links with other elements in NetForce. This means that each element in NetForce has different relationships, ties, with other elements in NetForce. And these relationships have an influence on the functioning of each element in NetForce. Some ties can become challenging or even threatening, when they are conflicting or when they decrease autonomy and hamper self-synchronisation. However ties can also be beneficial and provide chances. Therefore, training and education of military personnel should not only be focused on creating awareness and understanding of interaction and collaboration in NetForce, but also on understanding the influence of multiple ties on their network and on managing the influence of those ties on their network. In other words, interaction and collaboration in NetForce not only require competencies related to networked collaboration, but also political, organisational and cultural sensitivity.

Moreover, training and education should be focused on the group dynamic process of emergent interaction and collaboration. Military nodes need to be educated and trained in the different types and levels of interaction they may have with different elements in NetForce: other nodes, temporary sub-networks, orchestrating elements and strategic coalitions. They need to have an understanding of how interaction and collaboration is formed, developed and transformed. In other words, military personnel need to be educated and trained in the four phases of interaction and collaboration[51], including how internal and external factors influence the course of these four phases. They also need to learn how leadership, decision-making and information sharing emerge in these interactions and collaborations and how they can exploit the benefits and minimise the risks of these interactions and collaborations.

In complex, dynamic mission environments Tactical Designing provides an alternative for the often linear process of design, planning and execution and supports decision-making in complex, dynamic and networked environments. Military personnel need to learn to think about planning and decision-making as an iterative process. This means that activities will often be planned and executed based on a purpose and an often incomplete strategy (tactical design), which is based on current, often partial understanding of the environment. Military personnel need to learn to switch their tactics or strategy towards a purpose when an improved situational understanding gives reason to do so. They need to learn to operate in a continuous process of doing, probing, learning and adapting in a complex, dynamic and networked mission environment. Furthermore, military personnel need to learn how to work with the Strategy Knotworking method that supports a dynamic, iterative and adaptive way of planning. Furthermore, military personnel need to be educated and trained in interorganisational negotiation to unleash the power of existent and often hidden connections and alternatives in NetForce. They also need to learn about the mechanisms of the negotiation process.

Interaction and collaboration, including negotiation, require information sharing in NetForce. Information sharing can be supported by information management. An important step for the Netherlands armed forces is to invest in IM capacity for the operational units. IM is the profession that must fulfil this prerequisite. This IM-capacity will probably first have to learn to work according to the planned, coordinated approach of IM. At the same time, investments must also be made in awareness among operational users. They must learn that in fact every user (as information producer and information consumer) forms part of IM and they have to act on it when making information available and building and maintaining an information profile. A next step, would be to educate and train military information managers in networking with other information managers (representing other communities), establishing procedural and/or technical interfaces between digital collaboration environments (or merging them). This will be crucial in a setting with various temporary sub-networks.

---

51. Positioning, shaping, executing and transforming.

6.9   Concluding remarks

In this chapter we have provided a broad overview of the implications of NetForce Command for the armed forces along the DOTMLPFI lines. We also performed an analysis of these implications, using a system thinking perspective, to structure the implications and to identify the most critical ones for implementation of NetForce, including related multipliers. The analysis resulted in four critical implications that require changes and developments on several DOTMLPFI lines to make NetForce Command a reality:

		EMPOWERMENT	MINDSET	INTERACTION AND COLLABORATION IN JIMP SETTING	COPING WITH COMPLEXITY, DYNAMICS AND UNCERTAINTY
DOCTRINE	expansion of C2 doctrine				
	Tactical Designing				
	shift from order to mandate				
ORGANISATION	more enabling role of armed forces				
MATERIAL	availability of robust, interoperable and secure ICT network				
	attention for 'fallback' procedures				
	diagnostic, predictive and prescriptive decision support				
LEADERSHIP	Ambidextrous leadership, including Enabling leadership				
	Collective Leadership				
PERSONNEL	ability to operate in a broader range of C2 implementations				
	ability to cope with a high level of uncertainty				
	awareness of different forms of harmonisation support				
	ability to cope with different degrees of empowerment				
	self assessment				
	ability to cope with complexity and dynamics of Mission Environment				
	ability to cope with pressure of making 'far-reaching' decisions				
	'probe-sense-respond'				
	mindset focused on harmonisation				

		EMPOWERMENT	MINDSET	INTERACTION AND COLLABORATION IN JIMP SETTING	COPING WITH COMPLEXITY, DYNAMICS AND UNCERTAINTY
INTER-OPERABILITY	development of IM capacity			■	
	dependence on interaction and collaboration			■	
	ability to assess advantages and disadvantages of interactions			■	
TRAINING & EDUCATION	education in a broad range of C2 implementations				■
	training and education in empowerment	■			
	training and education in leadership, decision-making and IM	■			
	training and education on group dynamics of emergent interaction			■	

Figure 43: Overview of critical implications and related implications along the DOTMLPFI lines.

Empowerment

Empowerment is a critical implication because it has multiple linkages with other implications such as the ability to cope with the complexity, dynamics and uncertainty of the mission environment; tactical designing; a shift from order to mandate; a more enabling role of the armed forces as parent organisation; collective leadership and the ability to operate in a broader range of command and control implementations, including the ability to cope with different degrees of empowerment.

Mindset

Mindset is a critical implication, because it drives changes and developments of many other implications. For the implementation of NetForce Command it is important to develop a mindset within the armed forces that can be characterised as a flexible and adaptive mindset. A mindset, in which it is accepted that:

- The armed forces as parent organisation can have an enabling role;
- Planning and decision-making in NetForce concerns tactical designing, a continuous process of doing, probing, learning and adapting in a complex, dynamic and networked mission environment, in which a strategy emerges gradually and is not predefined;
- Military elements in NetForce receive mandates instead of detailed orders;
- Military elements in NetForce can influence but not command and control other elements in NetForce and therefore need to focus on harmonisation and a mutual gain in their negotiations;
- Collective leadership can exist alongside unity of command related to decision-making and command.

Interaction and collaboration in a JIMP setting

Interaction and collaboration in a JIMP setting is a critical implication, because it is the basis of NetForce Command in current and future operations and a multiplier for contributing effectively to a NetForce. Interaction and collaboration in a JIMP setting has linkages with implications such as the availability of a robust, interoperable and secure network; the development of information management capacity; awareness of different types and levels of interaction; the ability to assess advantages and disadvantages of interactions; the understanding of group dynamics in emergent interaction; a mindset focused on harmonisation; and collective leadership. In other words, developments related to interaction collaboration will also influence these other implications, including the required changes and developments for these implications.

Coping with complexity, dynamics and uncertainty of mission environments

Coping with complexity, dynamics and uncertainty of mission environments is a critical implication, because it determines the effectiveness of NetForce Command. Development of coping behaviour related to complexity, dynamics and uncertainty will also influence the development and changes related to implications such as tactical designing and the shift from orders to mandates; the enabling role of the armed forces as parent organisation; a robust, interoperable and secure ICT network, including fallback procedures and decision support; ambidextrous and collective leadership; self-assessment; negotiation and a focus on harmonisation; and the ability to operate in and switch between a broad range of command and control implementations.

By focusing developments of the armed forces along the DOTMLPFI lines of these four critical implications, we believe NetForce Command has the potential to function effectively in future missions and will be a mature alternative for hierarchical command and control in complex, dynamic and networked mission environments.
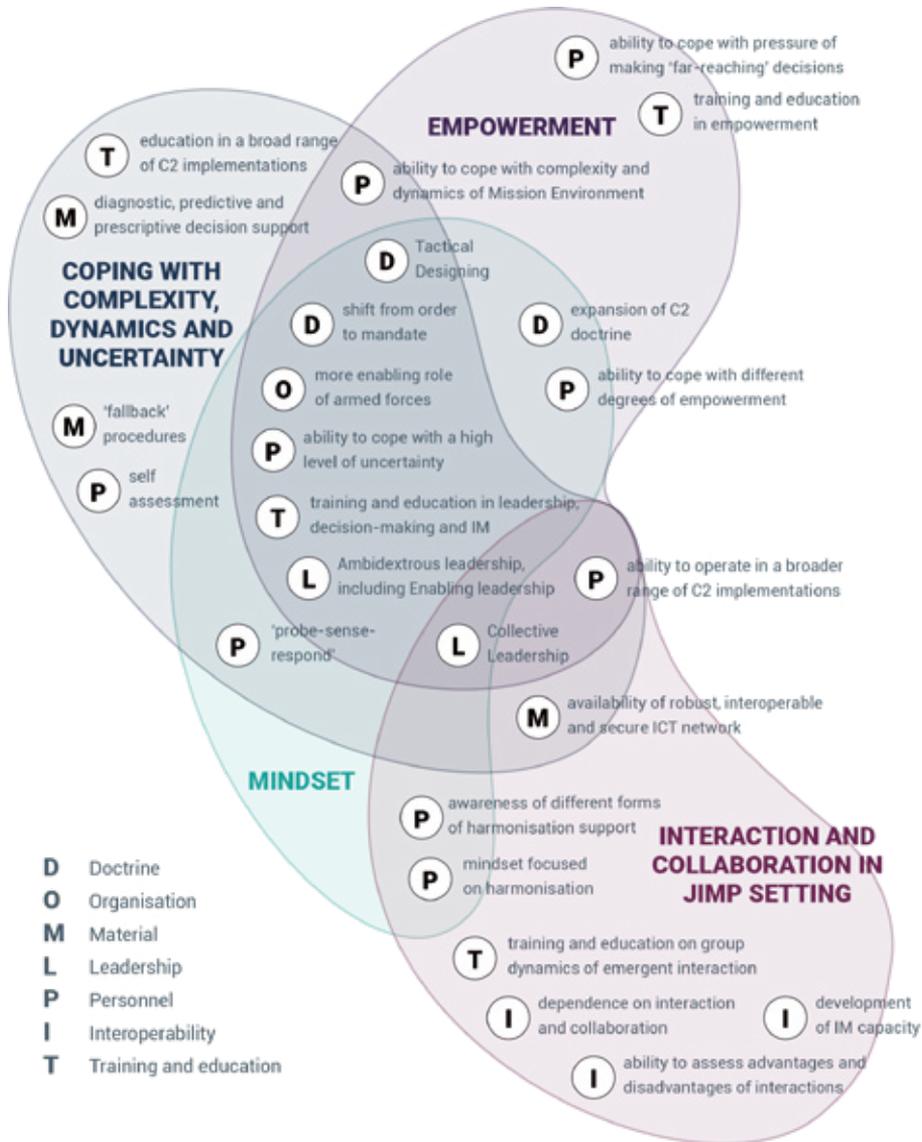
Figure 44: Four critical implications of the implementation of NetForce Command including their interrelations

REFERENCES

7

REFERENCES

Adaptable. *In Merriam-Webster's online Learner's Dictionary.* Retrieved from http://www.learnersdictionary.com/definition/adaptable, October 31, 2019.

Alberts, D.S., Gartska, J. J., Stein, F. P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority.* 2nd Edition (Revised). Washington, DC: CCRP Publication series.

Alberts, D.S. & Hayes, R.E. (2003). *Power to the Edge, Command & Control in the Information Age.* Washington, DC: CCRP Publication Series.

Alberts, D.S. & Hayes, R.E. (2006). *Understanding Command and Control.* Retrieved from http://www.dodccrp.org/html2/pubs_pdf.html, 12 April 2006.

Araki, L. M. K. (1999), *Self-synchronisation: What Is It, How Is It Created, and Is It Needed?* Working paper. Naval War College, Newport, RI.

Arquilla, J. & Ronfeldt, D. (2000). *Swarming and the Future of Conflict.* Santa Monica: RAND Corporation.

Australian Ministry of Defence (2009), *Army's Future Land Operating Concept.* Head Modernization and Strategic Planning: Army Australian Headquarters.

Beach, L. R. & Mitchell, T. R. (1990), *Image theory: A behavioural theory of decisions in organizations.* In: B. M. Staw & L. L. Cummings (Eds.), Research in organizational behaviour (Vol. 12). Greenwich, CT: JAI.

Beautement, P. (2006). *Agile and Adaptive Coalition Operations - Leveraging the Power of Complex Environments.* Paper presented at 11th International Command and Control Research and Technology Symposium (ICCRTS), 2006, 26-28 September, Cambridge, United Kingdom. http://internationalc2institute.org/proceedings.

Bemmel, I.E. van & Boor, R.A.E. van der (2019). V1604 *Leadership in NetForce; concept for leadership in complex, dynamic and networked environments.* TNO report: TNO 2018 R11308, Soesterberg: TNO.

Bemmel, I.E. van, Eikelboom, A.R. & Hekken, M.C. van (2019). V1604 *Decision-making in NetForce; concept for decision-making in complex, dynamic and networked environments.* TNO report: TNO 2018 R11309, Soesterberg: TNO.

Bemmel, I.E. van, Eikelboom, A.R., Hekken, M.C. van, Benda, R., Roelofs, M,L., Pieneman, R., & Kuijt, J.T. van de (2017). *NetForce Command, the next step?!.* Paper presented at 22nd International Command and Control Research and Technology Symposium (ICCRTS) 2017, 6-8 November, Los Angeles, California (USA). http://internationalc2institute.org/proceedings.

Benda, R., Bemmel, I.E., Vink, N., Hekken, M. van, Streefkerk, J.W., Kuijt, J. van de & Paulissen, R. (2017). *Towards the analysis, development and evaluation of NetForce Concepts, A framework to realise NetForce concepts in tomorrow's battlespace.* Paper presented at 22nd International Command and Control Research and Technology Symposium (ICCRTS) 2017, 6-8 November, Los Angeles, California (USA). http://internationalc2institute.org/proceedings.

Benda, R. & Vink, N. (2017). *Towards Hybrid Swarming, an investigation into the Theoretical Concept of Swarming in both the Physical, Information and Human Landscape.* TNO report: TNO 2017 R11513. Den Haag: TNO.

Benda, R., Hekken, M.C. van, Pieneman, R. & Michel, M. (2019). V1604 *NetForce informatievoorziening en informatiemanagement.* TNO report: TNO 2018 R11566. Soesterberg: TNO.

Benda, R., Hekken, M.C. van, Pieneman, R. (2014). *IMnibus – TNO Uitwerking van informatiemanagement binnen Defensie.* TNO publication (in cooperation with Dutch Ministry of Defence). Den Haag: TNO

Benda, R., Hekken, M. van & Ziekenoppasser, L. (2018). *V1604 C2 of Hybrid Swarming.* TNO report: TNO 2018 R11389. Den Haag: TNO.

Brown, M.E. & Gioia, D.A. (2002). Making things click. Distributive leadership in an online division of an offline organisation. *The Leadership Quarterly, 13, 397-419.*

Cebrowski, A. K. & Gartska, J. J. (1998). *Network Centric Warfare: Its Origin and Future.* Retrieved from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm

Chahine, S., Cristancho, S., Padgett, J., & Lingard, L. (2017). How do small groups make decisions? *Perspectives on medical education, 6(3), 192-198.*

Cottone, R.R. (2001). A social constructivism model of ethical decision-making in counselling. *Journal of Counselling and Development, 2001; 79(1), p. 39–45.* doi: 10.1002/j.1556-6676.2001.tb01941.x.

Cottone, R.R. (2004). Displacing the psychology of the individual in ethical decision-making: The social constructivism Model. *Canadian Journal of Counselling, 2004, 38(1): 5.*

Dalen, J.A. van (2008). *Swarming, Informatiebulletin 07/03.* Amersfoort: Education & Training Command, the Netherlands Armed Forces.

Dalen, van, J.A. Kol, Dekkers, P.A.P. Lkol and Daalen, A.F. van (2017). NetForce: een nieuw model voor toekomstige Defensie: 'Unleash the Power of the Netted Force'. *Militaire Spectator, 186 (3),* 125-140.

Dalenberg, S., Folkerts, I. en Bijlsma, T. (2014). Nieuwe Defensievisie leidinggeven. Op koers met het leiderschapskompas. *Militaire Spectator, 183 (1),* 26-39.

DeRue, D.S. & Ashford, S.J. (2010). Who will lead and who will follow? A social process of leadership identity construction in organisations. *The Academy of Management Review, 35, 4.*

Duijnhoven, H., Herder, A. & Sassen, J. (2017). *Theorie en praktijk van ambidexteriteit voor de Nederlandse Defensieorganisatie.* Retrieved from https://www.tno.nl/media/10745/ambidexterity-voor-de-nl-krijgsmacht.pdf.

Edwards, S.J.A. (2004). *Swarming and the Future of Warfare.* Santa Monica: RAND Corporation.

Eikelboom, A.R., Kuijt, J.T. van de, Benda, R., Pieneman, R. & Bemmel, I.E. van (2018). *Self-synchronization as additional approach to traditional C2.* Paper presented at 23rd International Command and Control Research & Technology Symposium (ICCRTS) 2018, 6-9 November, Pensacola, Florida (USA). http://internationalc2institute.org/proceedings.

Eikelboom, A.R., Koning, L., Hekken, M., Kamphuis, W., & ten Brake, G. (2016). *NTP iCOBUS.* TNO report: TNO 2017 R10320. Soesterberg: TNO.

Fair, M., Connaughton, S. & Daly, J. (2004). *Leading from afar - Leadership Training Challenges for Network Centric Warfare.* Paper (No. 1652), presented at the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2004.

Gonzales D., Johnson, M., McEver, J., Leedom, D., Kingston, G., Tseng, M. (2005). *Network-Centric Operations Case Study. The Stryker Brigade Combat Team.* USA, CA: RAND.

Hart, 't, M., Dekkers, P., Kamphuis, W., Sassen-van Meer, J., Vries, de, T. (2016). Het vergroten van adaptiviteit bij Defensie, *Militaire Spectator,* 185, 7/8, 320-335.

Hogan, R., Curphy, G. J., & Hogan, J. (1994). What we know about leadership: Effectiveness and personality. *American Psychologist,* 49(6), 493-504.

Hutchins, S. G., Kleinman, D. L., Hocevar, S. P., Kemple, W. G., Porter, G. R. (2001). *Enablers of Self-synchronisation for Network-Centric Operations: Design of a Complex Command and control Experiment.* Paper presented at 6th International Command and Control Research & Technology Symposium (ICCRTS) 2001, 19-21 June, United States Naval Academy, Annapolis, MD (USA). http://internationalc2institute.org/proceedings.

Kalkman, J. P., Kerstholt, J. H., & Roelofs, M. (2018). Crisis response team decision-making as a bureau-political process. *Journal of Contingencies and Crisis Management,* 26(4), 480-490.

Kamphuis, W, Dongen van, K, Thönissen, F, Zinc, M, Eikelboom, A, Essens, P. (2014), iCOBUS- *Intelligent support for multidisciplinary partnerships.* TNO report: TNO 2013 R11770. Soesterberg: TNO.

Keus, H.E. (2005). *Netforce Principles: An Elementary Foundation of NEC for Creating Joint Netcentric Environments.* Paper presented at 10th International Command and Control Research & Technology Symposium (ICCRTS) 2005, 13-16 June, McLean, Virginia (USA). http://internationalc2institute.org/proceedings.

Kuijt, J. van de, Bemmel, I.E. van, Benda, R, & Roelofs, M. (2019). V1604 *Functioning of orchestrating elements in NetForce: a blueprint.* TNO report TNO 2018 R11450. Den Haag: TNO.

Kuijt, J.T., van de, Eikelboom, A.R., Benda, R., Pieneman, R. (2017) V1604 *Self-synchronisation and orchestration as alternative approaches to traditional C2.* TNO report: TNO 2017 R11573, Den Haag: TNO.

Land Warfare Centre (2014). *Landoperaties; Doctrine Publicatie 3.2.* Amersfoort: auteur.

Land Warfare Centre (2015). *Deducties voor het landoptreden: editie Silene.* Amersfoort: auteur.

Land Warfare Centre (2017). *Future Land Operating Concept: Ascalon edition.* Amersfoort: auteur.

McCandless K. & Schartau, J. (2018). *Liberating Strategy. Surprise and Serendipity Put to Work.* Retrieved from http://www.liberatingstructures.com/km-articles/

Mouzas, S. & Ford, D. (2003). Negotiating in Networks: Unleashing the Power of Options. *Journal of Customer Behaviour, 2003, 2, p.2-20.*

Pearce, C. L., & Conger, J. A. (2003). *Shared leadership: Reframing the hows and whys of leadership.* Thousand Oaks, CA: Sage.

Raisch, S., & Birkinshaw, J. (2008). Organisational ambidexterity: Antecedents, outcomes, and moderators. *Journal of management,* 34(3), 375-409.

Rietjens, S. J. H. (2008). Managing Civil-Military Cooperation: Experiences from the Dutch Provincial Reconstruction Team in Afghanistan. *Armed Forces and Society,* 34, 173-207.

Ring, P. S. & Van de Ven, A.H. (1994). Developmental Processes of Cooperative Interorganisational Relationships. *The Academy of Management Review,* 19, 90-118.

Roelofs, M.L., Bemmel, I.E. van, Kalkman, J.P. & Kerstholt, J.H. (2018). *The influence of multiple ties on networked collaboration and decision-making.* TNO report: TNO 2018 R10563, Soesterberg: TNO.

Roelofs, M.L., Hekken, M.C. & Vos, P.M. (2019). V1604 *NetForce Collaboration – characteristics of collaboration in temporary sub-networks.* TNO report: TNO 2018 R11415, Soesterberg: TNO.

Roelofs, M.L., Kerstholt, J., & van Bemmel, I.E. (2017). *Networked collaboration: lessons learned from the civilian domain.* Paper presented at 22nd International Command and Control Research and Technology Symposium (ICCRTS) 2017, 6-8 November, Los Angeles, California (USA). http://internationalc2institute.org/proceedings.

Rosing, K., Frese, M., & Bausch, A. (2011). Explaining the heterogeneity of the leadership-innovation relationship: Ambidextrous leadership. *The Leadership Quarterly,* 22(5), 956-974.

Royal Netherlands Army (2018). *Exercise Deep Strike 2018.* Havelte: auteur.

Spiegeleire, de, S., Sweijs, T., Jong, de, S., Oosterveld, W., Rõõs, H., Bekkers, F., Usanov, A., Rave, de, R., & Jans, K. (2017). *Volatility and Friction in the Age of Disintermediation,* Strategic Monitor 2016-2017 Annual Report. The Hague: HCSS.

Sweijs, T., Bekkers, F. and Spiegeleire S. de (2018). *Playing your strengths: A different perspective on future capabilities for the Royal Netherlands Army,* HCSS Security Report. The Hague: HCSS.

The Netherlands Ministry of Defence (2017). *Zicht op Gereedheid.* Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2017/03/12/zicht-op-gereedheid

The Netherlands Ministry of Defence (2012). *Joint Doctrine Publicatie 5: Commandovoering.* Den Haag: auteur.

Tjemkes, B., Vos, P., Burgers, K. (2012). *Strategic Alliance Management.* London, UK: Routledge.

Tuckman, B. W. (1965). Developmental sequence in small groups. *Psychological Bulletin,* 63, 384–99.

Uhl-Bien, M., Riggio, R. E., Lowe, K. B., & Carsten, M. K. (2014). Followership theory: A review and research agenda. *The Leadership Quarterly,* 25(1), 83-104.

Uhl-Bien, M. & Arena, M. (2018). Leadership for organisational adaptability: A theoretical synthesis and integrative framework. *The Leadership Quarterly 29* (2018), 89–104.

Whelan, C. (2015). Managing Dynamic Public Sector Networks: Effectiveness, Performance, and a Methodological Framework in the Field of National Security. *International Public Management Journal, 18*(4), 536-567.

Zweibelson, B. (2015). An awkward tango: Pairing traditional military planning to design and why it currently fails to work. *Journal of Military and Strategic Studies, 16 (1).*

Zweibelson, B. (2017). Blending postmodernism with military design methodologies: Heresy, subversion, and other myths of organizational change. *Journal of Military and Strategic Studies, 17 (4).*

ANNEX A
NetForce Command Research Programme

The objective of the NetForce Command research programme is to develop operational, netcentric concepts for organisation, interaction and collaboration, command, leadership, decision-making, and information management and to aggregate these concepts into an integrated NetForce Command concept that provides the Dutch defence organisation with the opportunity to contribute and operate effectively in a complex, dynamic and networked mission environment. To be able to develop these operational, netcentric concepts we also developed a potential operating concept (hybrid swarming) to get an understanding of the functioning and implementation of a NetForce and to support the development of the NetForce Command concept. The lead time of the research programme was four years and consisted of three phases:

• Phase 1: Orientation on NetForce Operations (2016)
• Phase 2: Concept Development and Experimentation (2017 and 2018)
• Phase 3: Concept Integration (2019)

Phase 1: Orientation on NetForce Operations (2016)
To get an understanding of what NetForce and NetForce operations are, an extensive military review was carried out, in which different views and cases of NetForce and related concepts were analysed and a NetForce framework was developed. Furthermore, a review was carried out on networked organisations and related concepts in a civilian context. Both reviews provided information on characteristics, challenges, preconditions, strengths and weaknesses of networks and networked organisations. Simultaneously an international reconnaissance was done in search of information on current or near future research programmes, literature (papers, proceedings, experiments...) and subject matter experts in other countries. Output of the literature reviews and international reconnaissance was combined in a first draft concept of NetForce Command, including

challenges and promising concepts for control, leadership, decision-making, organisation, collaboration and information-sharing. These challenges and promising concepts formed the starting point for the concept development and experimentation phase.

Phase 2: Concept Development and Experimentation (2017 and 2018)

Based on the challenges and promising concepts from the literature reviews and international reconnaissance, NetForce Command concepts were developed for organisation, collaboration, command, leadership, decision-making, and information-management and discussed during workshops and in interviews with subject matter experts. Furthermore, we developed and experimented with a potential operating concept for NetForce to get an understanding of the functioning of a NetForce and to support the development of the NetForce Command concept. The NetForce Command concepts formed the input for phase 3.

Phase 3: Concept Integration (2019)

The concepts that were developed in phase 2 were integrated in a NetForce Command concept. Furthermore, we conducted a project to determine the implications of the NetForce Command concept for operational readiness: personnel readiness, materiel readiness and combat readiness. In this project we also explored the implications for operational logistics, communication and information systems and tactical operations.

ANNEX B NETFORCE COLLABORATION FRAMEWORK

NetForce Element Type

Type of Element

Nodes | Parent organisations | Temporary sub-networks | Orchestrating elements | Strategic coalitions

Function and Purpose

Common objective
The objective of the NetForce element.

Function
(more than one function may be applicable)

Shared situational understanding | Design | Planning | Execution

Reason to participate
The reason(s) for the nodes / parent organisations to participate in the interaction/collaboration. (not applicable for a single node)

Intended level of interaction (internal interaction)
The level of interaction between the (representatives of the) nodes / parent organisations. (not applicable for a single node)

Level 0 Unawareness | Level 0,5 Awareness | Level 1 De-confliction | Level 2 Coordination | Level 3 Collaboration | Level 4 Integration

Intended level of orchestration (external interaction
The level of interaction between the orchestrating NetForce element and the orchestrated NetForce elements. (only applicable for orchestrating elements and strategic coalitions)

Low ———————————— High

Origin
The formation of a NetForce element: top-down or bottom-up. (not applicable for a single node)

Bottom-up ———————————— Top-down

Composition

Size
The number of nodes in a NetForce element. (not applicable for a single node)

Small S ———————————— L Large

Level of diversity
The diversity of nodes (capabilities) in a NetForce element. (not applicable for a single node)

Homogeneous ———————————— Heterogeneous

Organisation and Structure

Organisation structure	The structural organisational design / form of a NetForce element. Networked ●⬦● ├────────────────┤ ⬥ Hierarchy
Control implementation	The type of monitoring and control applied within the NetForce element. (not applicable for a single node or self-sync interaction level 0-2)
Leadership implementation	The type of leadership applied within the NetForce element. (not applicable for a single node or self-sync interaction level 0-2)
Decision making implementation	The type of decision making applied within the NetForce element. (not applicable for a single node or self-sync interaction level 0-2)
Information sharing implementation	The type of information sharing and information management applied within the NetForce element: which information sharing and information management concepts are applied?
Work agreements	The procedures, mechanisms, etc. that are applied in a NetForce element to perform activities.
Digital support	The tools, applications, communication means, etc. that a NetForce element needs to perform activities.

Culture

Degree of formalisation	The extent to which work roles are structured in a NetForce element, and to which the activities are governed by rules and procedures. Formal ├────────────────┤ Informal
Orientation	The extent to which a NetForce element is open to external new and innovative ideas and is focused on its contribution in the external environment (in contrast to a focus on internal ideas, procedures and development). Internal ├────────────────┤ External
Adaptibility	The extent to which a NetForce element is able to adapt its performance to changes in the mission environment and to the need of other nodes in NetForce. Robust ├────────────────┤ Agile
Openness	The difficulty of getting in and out of the NetForce element. (not applicable for a single node) Closed ├────────────────┤ Open
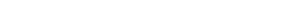
Behaviour (external)

Style of orchestration (only applicable for orchestrating elements and strategic coalitions)	The orchestration style that the NetForce element exposes to the orchestrated NetForce elements. This orchestration style / behaviour may be described in terms of control, leadership and decision making. (only applicable for orchestrating elements and strategic coalitions) Supporting ├────────────────┤ Control

ACKNOWLEDGEMENTS

NetForce Command
An alternative for hierarchical command and control
in complex, dynamic and networked mission environments

TNO
Oude Waalsdorperweg 63
2509 JG The Hague
TNO.NL

Authors
Ingrid van Bemmel: ingrid.vanbemmel@tno.nl
Marcel van Hekken: marcel.vanhekken@tno.nl
Aletta Eikelboom: aletta.eikelboom@tno.nl
Judith van de Kuijt: judith.vandekuijt@tno.nl
Roy Benda: roy.benda@tno.nl
Rosie Paulissen: rosie.paulissen@tno.nl
Lisa Ziekenoppasser: lisa.ziekenoppasser@tno.nl

Design
PI&Q graphic design

NetForce Command provides an alternative for the hierarchical approach of command and control and is developed specifically for complex, dynamic and networked environments, in which a high operational tempo, agility and harmonisation of the efforts of multiple military and civilian actors are essential. NetForce Command is a networked approach of command in which collaboration and information sharing are paramount and the function of command is (informally) shared with or distributed between military and civilian capabilities contributing to a NetForce. NetForce Command is not to replace a hierarchical approach of command and control, but intents to broaden the range of command and control approaches that the armed forces can apply.

This book provides the building blocks for the expansion of current command and control doctrine and the implementation of NetForce Command. The book can be read as a NetForce and is meant to inspire, to stimulate further conceptual thinking about NetForce Command and to encourage experimentation with different aspects of NetForce Command. In a way, you can swarm through the book and begin your own NetForce Command thought experiment.

TNO innovation for life