

Chapter 3

Networked Operations: Taking into Account the Principles of Modular Organizing

E. J. de Waard

Netherlands Defence Academy, The Netherlands

ABSTRACT

Decentralized, peer-to-peer command and control is a key principle of network-centric operations that has received a lot of scholarly attention. So far, robust networking, another principle, has remained rather underexposed in the academic debate. This chapter introduces theory on modular organizing to start a discourse on network robustness from an organizational design perspective. Above all, the chapter makes clear that the level of system decomposition influences the command and control process of composite military structures. When military organizations follow a fine-grained modularization approach, the structure of a task force deployed may become complex, asking for extra coordination mechanisms to achieve syntheses between the many contributing functional organizational components. In addition, it is argued that modularity's principle of near-decomposability has to be incorporated into the available mathematical models on network-centric operations. A point of concern, in this respect, is that the current modeling parameters make no clear distinction between the different types of actors—or nodes—in a military network structure, whereas in reality, technological, organizational, and human actors all live by their own specific rules.

INTRODUCTION

Since the mid 90s we have witnessed a change process within most Western militaries to improve organizational responsiveness, which is based upon fine-grained organizational cooperation, supported by the possibilities of modern-day information and communication technology (ICT). The United States and its European allies have

respectively introduced Network Centric Warfare (NCW) and Network Enabled Capabilities (NEC) as the underlying concepts of their new doctrines. Both NCW and NEC propagate fundamental changes in the Command and Control (C2) process (Alberts, Garstka, & Stein, 2000). In the current dictionary of military and associated terms C2 is defined as: “The exercise of authority and direction by a properly designated

DOI: 10.4018/978-1-4666-6058-8.ch003

commander over assigned and attached forces in the accomplishment of the mission” (JP 1-02, p.47). Interesting about this definition is its quite traditional commander-centric focus, whereas NCW and NEC strongly broadcast the idea of peer-to-peer decision-making.

An important viewpoint in today’s literature on NCW and NEC is that decentralized decision-making can only take shape when military organizations adopt a different type of organizational structure. Where the abovementioned definition makes clear that the paradigm of a centralized and hierarchical structure still dominates military practice, NCW/NEC advocates argue that Mintzberg’s (1983) structural typology of the adhocracy better suits network-centric conditions (Alberts & Nissen, 2009). Especially, the ability to exploit network effects is more naturally incorporated into an adhocracy compared to a centralized hierarchy. However, since Mintzberg’s adhocracy is a rather broadly defined organizational configuration, the NCW/NEC community has developed a toolkit, known as ELICIT, to translate the general organizational principles of the adhocracy into concrete organizational mechanisms that facilitate a decentralized C2 approach. As the title of Alberts and Hays (2003) book *Power to the Edge* indicates, simulation using the ELICIT toolkit shows that a structure – the edge organization – that avoids pre-assigned leaders and functional grouping offers more agility than the traditional hierarchy (Thunholm, et al., 2009).

Notwithstanding, the ELICIT program primarily concentrates on the relationship between organizational design parameters and decision-making. The connection between robust networking, which is also presented as one of NCW/NEC tenets (Alberts & Hayes, 2003), and specific organization design rules remains largely untouched. While, it could be argued that robust networking entails more than a decentralized, peer-to-peer process of decision-making. Kleindorfer and Wind (2009: 5) state that “A network may be defined mathematically as a set of nodes and arcs that connect

specific pairs of these nodes. These interlinked structures serve as conduits for information, human resources and capital, material flows, and associated risks.” Based on this definition it could be argued that the ELICIT program only lifts a corner of the networking veil. The principle of avoiding pre-assigned leadership and functional grouping relates to a certain degree to the composition of and interaction between nodes in a network. However, many important aspects of network robustness still remain unanswered. For example, ELICIT argues that functional grouping should be avoided, whereas many military task forces are by nature functionally grouped into specific task domains such as maneuver, combat support, combat service support, command and control, etc. Moreover many major military operations have a multi-national and multi-service character. The organizational dynamics of this reality of intra and inter organizational collaboration has not been explicitly addressed by the ELICIT program. This chapter aims to contribute to bridging this gap by digging into the principles of modular organizing.

The reason for focusing on the variable modular organizing is threefold. First, military transformation literature explicitly mentions modularity as the underlying organizational approach of military task force design (Dandeker, 2003). Second, organization and management theory (OMT) presents ‘modular organizing’ – or modularity – as a typical organizational design strategy to increase flexibility without jeopardizing operational performance. By using fixed, self-supporting, autonomous organizational modules and by controlling only the required output of these modules, a loosely coupled system is created that can be reconfigured into customized constellations (Sanchez, 2003; Schilling & Steensma, 2001; Worren, Moore, & Cardona, 2002). Third, as yet the military network modeling community makes no clear distinction between the different types of nodes in a network. Available insights from OMT on organizational modularity could offer some valuable preconditions for the modeling of military units within

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/networked-operations/109732

Related Content

Applications of Computational Intelligence to Impairment-Aware Routing and Wavelength Assignment in Optical Networks

Joaquim F. Martins-Filho, Carmelo J. A. Bastos-Filho, Daniel A. R. Chaves and Helder A. Pereira (2013). *Intelligent Systems for Optical Networks Design: Advancing Techniques* (pp. 194-216).

www.irma-international.org/chapter/applications-computational-intelligence-impairment-aware/77110

Hyper Connectivity as a Tool for the Development of the Majority

Danilo Piaggese (2021). *International Journal of Hyperconnectivity and the Internet of Things* (pp. 63-77).

www.irma-international.org/article/hyper-connectivity-as-a-tool-for-the-development-of-the-majority/267223

Security Policy Specification

Jorge Bernal Bernabé, Juan M. Marín Pérez, Jose M. Alcaraz Calero, Jesús D. Jiménez Re, Félix J.G. Clemente, Gregorio Martínez Pérez and Antonio F.G. Skarmeta (2013). *Network and Traffic Engineering in Emerging Distributed Computing Applications* (pp. 66-93).

www.irma-international.org/chapter/security-policy-specification/67499

A Brief Study on Smart Medicine Dispensers

Dayananda P., Amrutha G. Upadhyay, Nayana B. G., Priyam Poddar and Vandana Rao Emaneni (2022). *International Journal of Hyperconnectivity and the Internet of Things* (pp. 1-7).

www.irma-international.org/article/a-brief-study-on-smart-medicine-dispensers/294893

SEF4CPSIoT Software Engineering Framework for Cyber-Physical and IoT Systems

Muthu Ramachandran (2021). *International Journal of Hyperconnectivity and the Internet of Things* (pp. 1-24).

www.irma-international.org/article/sef4cpsiot-software-engineering-framework-for-cyber-physical-and-iot-systems/267220