Chapter 7
Dynamical Network Structures in Multi-Layered Networks: Implementing and Evaluating Basic Principles for Collective Behavior

R. H. P. Janssen
Netherlands Defence Academy, The Netherlands

H. Monsuur
Netherlands Defence Academy, The Netherlands

A. J. van der Wal
Netherlands Defence Academy, The Netherlands

ABSTRACT

In modeling military (inter)actions and cooperation as networks, military units or actors may be represented as nodes. In analyzing military networked action, a key observation is that a node is not just part of one type of network but simultaneously belongs to multiple networks. To model the dynamical behavior of actors, one has to take into account the interdependence of the different networks. In this chapter, the authors present a method that is used to implement, analyze, and evaluate some specific principles that may be used by the actors in an organization to drive the process of constant change. It can be used to analyze the effect of these principles on the metrics for coordination, synchronization, robustness, and desired operational effectiveness of the network as a whole. To demonstrate the approach, the authors apply it to networks in which two basic principles are operational: reciprocity and a novel principle called covering.

DOI: 10.4018/978-1-4666-6058-8.ch007

INTRODUCTION

Background / Motivation

Military operations have grown increasingly complex over the past years. Modern operations are non-conventional, involving missions like counterterrorism, peacekeeping and crisis management. Characteristics of these operations include the participation of many stakeholders, each with their own objectives and involving multiple chains of command, rapidly changing environments, short reaction times and increased uncertainty concerning the operating environment or theatre area. In addition to these complexities, the enemy or opponent operates in a networked manner. They are connected through complex social, informational and physical networks that dynamically adapt to the environment. Outmaneuvering such an intelligent opponent is a daunting task. As General McChrystal (2011) put it: "it takes a network to defeat a network."

Given these complexities and challenges, it is of paramount importance that the units of a defense organization are also connected through multiple social, informational and physical networks. This coupling enables military units to coordinate and synchronize their individual actions with one another to achieve greater operational effectiveness. These insights triggered the development of the concepts of Network Centric Warfare (NCW) in the mid-1990s, later named Network Centric Operations (NCO) in the US and Network Enabled Capabilities (NEC) within NATO. These concepts involve the use of complex, networked systems, consisting of many components that are heterogeneous in functionality and capability with both nonlocal and non-linear interactions and effects, cf. Alberts et al., 1999; Cares, 2005; Monsuur, Grant and Janssen, 2011. It is now widely accepted that C2 systems are socio-technical in nature. In addition to the technical infrastructure in the form of supporting computing and telecommunication networks, the analysis also centers on the inter-relationship between doctrine, organization, training, material, leadership, personnel, facilities (DOTMLPF). This view induces a transformation of C2 systems from a rigid, hierarchical organizational structure towards an agile networked organizational form. In this case one assumes that information sharing, collaboration and self synchronization ultimately lead to increased mission effectiveness (an element of the so-called NEC value chain). As described in McChrystal (2011), lessons learned from recent operations show that, in addition to being connected, the organizational form also has to be dynamic. To be agile and be able to react adequately to varying conditions, a constantly changing, adapting operational social and information network has to be the hallmark of a modern defense organization or crisis management team. As also illustrated by other research (for example, see Alberts, 2011), various heterogeneous networked units are needed to ensure agility and mission effectiveness. This process of constant change, if restricted to social and information networks, has several characteristics (see McChrystal, 2013). First of all, change is not centrally orchestrated and units may, to a degree, be considered as autonomously acting agents. Change is neither meant to create the most efficient bureaucratic model nor is it a process of optimizing for variables that have become irrelevant. Secondly, as is the case with the competitors, there is neither an organizational end-state, nor advance knowledge of the next state. Finally, change has to be guided by a few basic principles. Meanwhile, one has to constantly monitor the health of the network by how well each unit shares a common understanding of the battlefield and the strategy to defeat an enemy or manage a crisis situation. This self-monitoring of the network as an enabler of C2 is necessary to be able to act both reactive and proactive. Finding the right basic principles that drive the process of change will be a learning process.

In this chapter, we present a method that can be used to implement, simulate, analyze and evalu-