Chapter 5
Formalized Ontology for Representing C2 Systems as Layered Networks

T. J. Grant
R-BAR, The Netherlands

ABSTRACT

Command and Control (C2) is an essential operating capability in which the commander exercises authority over assigned forces to accomplish the mission. Traditionally, military C2 was organized hierarchically with the commander issuing directives top-down and subordinates reporting progress upwards. Over the past two decades, developments in digital telecommunication technology have made it possible to link distributed computer systems into a network. These developments can be exploited to delegate decision-making authority down the organizational hierarchy. Subordinates can be empowered to share information and synchronize their actions with their peers, speeding up the response to changes in the situation. This is known as Network-Enabled Capabilities or information-age C2. Experience has shown that multiple factors must co-evolve to gain the full benefit of transforming C2 to become network enabled. In this chapter, the authors group these factors into five layers: geographical, physical, information, cognitive, and socio-organizational. They formalize the key entities in each layer, together with within- and across-layer relationships, into a conceptual ontology, known as the Formalized Layered Ontology for Networked C2 (FLONC). To ensure the ontology is militarily relevant, the authors show that a set of networks found in military operations can be extracted from the ontology. Finally, they compare the formalized ontology to related work on ontologies in C2. In further research, the ontology could be used in developing software to simulate and support network-enabled C2 processes. A case study based on the events of September 11, 2001 shows how this could be done.

DOI: 10.4018/978-1-4666-6058-8.ch005

INTRODUCTION

Background

Command & Control (C2) is one of NATO's Essential Operating Capabilities. It is defined as "*the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission*" (US DoD Joint Publication 1-02, 2013). A C2 system is "*an arrangement of personnel, equipment, communications, facilities, and procedures*", and the functions of C2 include "*planning, directing, coordinating, and controlling forces and operations*" (ibid.) These definitions show that C2 is not confined to the technical implementation. The definition hints at organization ("*authority and direction*", "*assigned and attached forces*", and "*personnel*"), knowledge ("*mission*", "*procedures*", and "*planning*"), and information ("*communications*", "*directing*", and "*coordinating*"), as well as technology ("*equipment*", "*communications*", and "*facilities*").

Traditionally, military C2 was top-down and directive, emphasizing achievement of the commander's intent (the "*mission*"), with subordinates (the "*assigned and attached forces*") periodically reporting their progress towards achieving this intent. This required a hierarchical organization, with communications passing up and down the hierarchy. Subordinate units report progress in the form of situation reports up the hierarchy, and commanders promulgate their intent down to their subordinates in the form of operation orders. In a hierarchical organization, subordinate units rarely communicate directly with one another (Van Fenema, Rietjens & Besters, 2014). Instead, the commander carries the burden of synchronizing their activities, usually by deconfliction, e.g. by giving them mutually exclusive areas of responsibility. The technical systems supporting this traditional C2 process were designed to mirror the organizational hierarchy. This has been termed "industrial-age" C2 (Alberts, 2002).

There are several shortcomings of industrial-age C2. Firstly, commanders suffer from information overload. Secondly, commanders can form a bottleneck in the information flow, both in synchronizing their subordinates' activities and in summarizing the reporting from subordinates in a report to their own superior. Thirdly, only the commander has an overview of the situation, often hampering subordinates in gaining an understanding of the rationale behind their commander's intent. Fourthly, the concentration of information at the commander's location makes him/her an attractive target for the enemy.

Over the past two decades, developments in digital telecommunication technology have made it possible to link distributed computer systems into a network. In 1998, Vice Admiral Cebrowski and John Garstka published an article in the US Naval Institute Proceedings outlining the concept of network-centric warfare (NCW) (Cebrowski & Garstka, 1998). Since then, NCW – now termed network-centric operations (NCO) in the USA and network enabled capabilities (NEC) in NATO, the UK, and the Netherlands – has been the subject of extensive research, concept development, experimentation, and operational application. (In this chapter, we will use NATO terminology.) NEC is based on four tenets (Alberts, 2002):

Tenet 1: A robustly networked force improves information sharing.

Tenet 2: Information sharing and collaboration enhance the quality of information and shared situational awareness.

Tenet 3: Shared situational awareness enables self-synchronization.

Tenet 4: These, in turn, dramatically increase mission effectiveness.

As the name suggests, NEC focuses on networks. At the outset, networking was overwhelmingly seen as a technological capability. By "network", one meant the telecommunication network that linked the C2 systems electronically. Gradually, as scientific and practical knowledge built up, it became apparent that an exclusively

Making IoT Run: Opportunities and Challenges for Manufacturing Companies
Peter Schott, Torben Schaft, Stefan Thomasand Freimut Bodendorf (2017). *International Journal of Hyperconnectivity and the Internet of Things (pp. 26-44).*
www.irma-international.org/article/making-iot-run/201095