19th International Command & Control Research & Technology Symposium

“C2 Agility: Lessons Learned from Research and Operations”

Advancing the State of the Art in Applying Network Science to C2

Paper ID 053

Topic(s)
Primary:

Topic 2. Organizational Concepts and Approaches

Alternate:

Topic 1: Concepts, Theory, and Policy

Names of Authors
Tim Grant, Herman Monsuur, & René Janssen

Point of Contact
Tim Grant

Retired But Active Researcher (R-BAR)

Koningin Wilhelminastraat 13, 3405 XP Benschop, The Netherlands

Tel: +31 (0)638 193 749

tim.grant.work@gmail.com

Abstract

The “modern period” of network science – the theory and application of network structure and behaviour – and Network Enabled Capabilities (NEC) – emerged in the mid to late 1990s. While NEC concentrated initially on telecommunication networks, network science was applied from the outset to modelling real-world phenomena as biological, technical, information, and social networks. Network scientists developed a range of theoretical instruments concerning the properties of nodes and networks, network topologies, robustness, and processes. While NEC researchers extended their coverage from technological networks to include information, cognitive and social networks, they have yet to apply the full range of theoretical instruments now available.

In early 2013, the authors of this paper commissioned a number of scientific contributions to a book (Grant, Janssen & Monsuur, 2014) aimed at connecting the fields of C2 and network science.

Researchers from the US, the UK, Australia, Sweden, and the Netherlands provided contributions covering applications ranging from the (cyber-) geography of C2, through physical, technical, information, and cognitive networks, to the socio-organizational level. The contributions advance the state of the art in applying network science to C2, but there are still large "white areas" where research needs to be done. This paper summarizes the contributions and makes recommendations for further research.

1. INTRODUCTION

Network science and network-enabled Command & Control (C2) both emerged in the mid- to late-1990s, although their roots are much older. Network science is a modern branch of mathematics and Operations Research (OR), with its roots in graph theory going back nearly three hundred years to Leonhard Euler's solution of the *seven bridges of Königsberg* problem. C2 is a branch of the military sciences closely associated with leadership, with a history of thousands of years going back to the ancient Greeks, if not longer. With the introduction of telecommunications over the past 180 years – first the telegraph, then the telephone and radio, and, most recently, the computer and computer networking – C2 has gained a strong engineering flavor.

Lewis (2009, p.9) defines network science as "*the study of the theoretical foundations of network structure/dynamic behavior and the application of networks to many subfields*", listing these as social network analysis, collaboration networks, synthetic emergent systems, physical science systems, and life science systems. Brandes, Robins, McCranie & Wasserman (2013, p.5) succinctly claim that "*theories about network representations and network theories about [real-world] phenomena*" both constitute network theory. There are two key elements in both definitions: theory and applications. From the theoretical viewpoint, a network is a set of nodes and a set of arcs linking these nodes to one another. From the application viewpoint, what networks, nodes, and arcs represent in the real world can vary widely. Vice versa, real-world applications can impose requirements on the mathematical representation and on how this representation is employed.

C2 is the process of monitoring, directing, and controlling assigned resources to achieve the mission, often in remote and perhaps dangerous environments (adapted from JP 1-02, 2013). Variants of this process are to be found in military operations, emergency management, disaster relief, and real-time process-control applications (e.g. transport, utilities, distribution, and logistics). C2 is invariably a team effort, often involving multiple organizations, supported by computers and telecommunications, each with their own doctrine, operating procedures, and norms of behaviour. Human qualities, such as leadership, are essential to C2, and will remain so for the foreseeable future. C2 involves the interplay between humans and machines, demanding that it be studied from a socio-technical systems viewpoint (Trist & Bamforth, 1951).

In applying the network representation to C2, the nodes may model individual people, teams, organizational units, vehicles, ships, aircraft, satellites, computers, hubs, routers, and more. The arcs can link people who know each other or who have family, tribal, or national relationships in common, yielding a *social network*. Alternatively, they can designate superior-subordinate relationships between people, teams, and organizational units, yielding an *organizational structure* (often depicted as an *organigramme*). From an engineering viewpoint, arcs may model the wired or wireless links over which computers, hubs, and routers exchange digital messages, yielding a *telecommunications network*. Operationally, road, rail, water, sewage, electricity, and other types of *physical network* may all have an important role to play in C2.

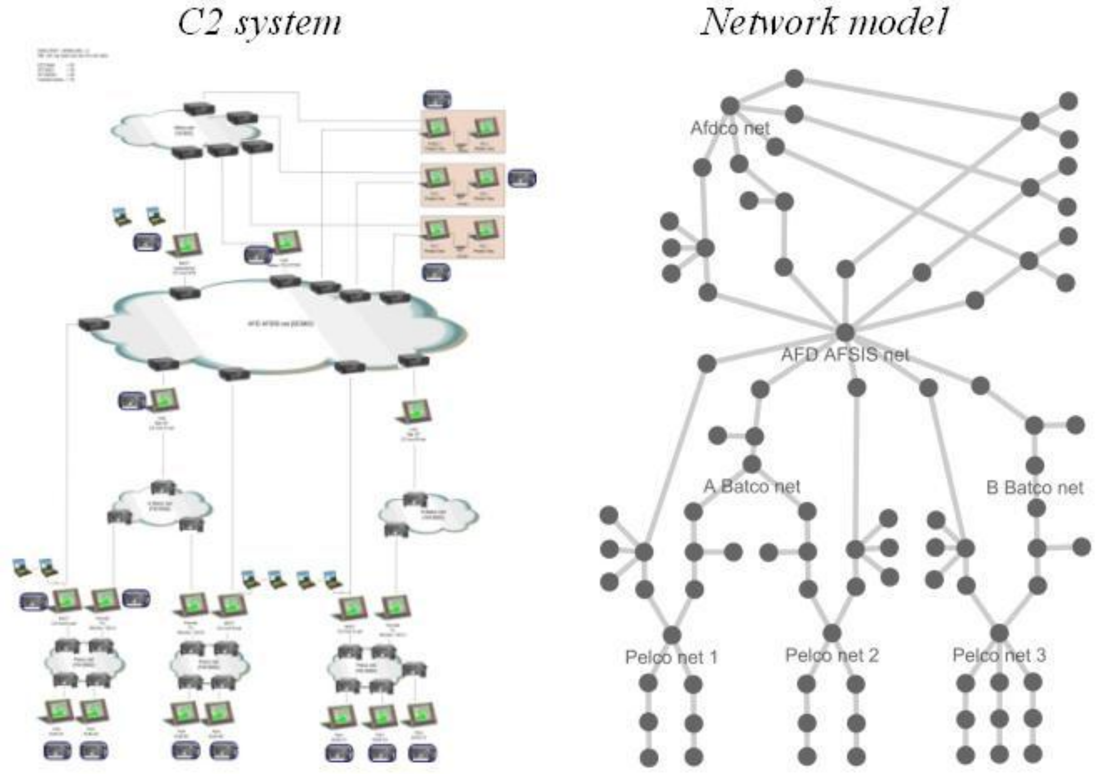

Figure 1. How C2 system (left) can be modelled (right) as network (Grant, Buizer & Bertelink, 2011).

To illustrate modelling real-world phenomena as networks, Figure 1 shows on the left a small C2 system used by the Royal Netherlands Army for training purposes. This consists of several groups of laptops and modems, connected partly by cabling and partly by radio nets (shown as “clouds”). This can be modelled as a network of nodes and arcs, as shown on the right. Each laptop and modem is modelled as a node (shown as a blob), and the connections as arcs. Each radio net is modelled as a node linked in a star pattern to the modems. Clearly, this model is an example of a telecommunications network.

Modern C2 systems link tens of thousands of computers and their users. With unmanned vehicles, sensors, and other devices being added daily, the number of C2 nodes is increasing exponentially. Modern network science provides the mathematical techniques for representing and analyzing networks with thousands and millions of nodes, i.e. for handling “big data”. In the mid-1990s, Cebrowski and Garstka (1998) introduced some of the concepts from network science into military operations in advocating a new C2 approach, known initially as *network-centric warfare* (NCW) and now known as *network-centric operations* (NCO) in the US and *network-enabled capabilities* (NEC) in Europe and NATO. Alberts and Hayes (1999; 2003; 2006; 2007) built extensively on these ideas at the conceptual level. Judging by when specific research initiatives were set up (as described in more detail in Section3), network science techniques have been applied to C2 from 2004 onwards, initially representing only the physical telecommunications network. Gradually, network science has been extended to the social networks of C2 users and their adversaries. Since 2009, network science has been applied to cognitive networks, i.e. the mental models in C2 users' minds. Until now, work has been largely focused on technical, communications, information, and social networks.

The two disciplines – network science and C2 – have developed separately, and have separate literatures. The academic communities are largely separate, with their own journals and conferences. There are books on C2, and books on network science, but no previous books have comprehensively applied network science to C2. There are scientific articles, some Masters and PhD theses, and at least one monograph (Cares, 2005) applying network science to C2, but these do not treat the subject comprehensively.

In early 2013, the authors of this paper commissioned a number of scientific contributions to a book aimed at connecting the fields of C2 and network science from a wide variety of viewpoints. Researchers from the US, the UK, Australia, Sweden, and the Netherlands provided contributions covering applications ranging from the (cyber-) geography of C2, through physical, technical, information, and cognitive networks, to the socio-organizational level. Case studies ranged from engaging citizens in searching for missing children, through a major fire in a chemical factory and an insurgency scenario, to Operation Unified Protector in Libya and the events of September 11th, 2001. Comparing these contributions to the pre-existing applications of network science to C2 shows that these researchers have made advances in extending applications upwards to represent organizations and coalitions. Above all, they have been successful in combining network science and C2 theory. However, there remain several "white areas" where further research is needed.

The purpose of this paper is to summarize the contributions and to place them into an analysis framework. The paper is divided into five sections. After this introductory section, section 2 reviews what has been achieved in the modern period of network science. Section 3 reviews the achievements made in applying network science to C2. Section 4 presents an analysis framework, summarizes the contributions, and identifies the advances made by placing the contributions into the analysis framework. Section 5 draws conclusions and makes recommendations for further work.

2. NETWORK SCIENCE

Lewis (2009) distinguishes three periods in the history of network science. After Euler's introduction of graph theory, it spent 200 years in the backwaters of arcane mathematics. It re-emerged in the 1950s when Paul Erdos investigated the mathematics of random graphs. In the 1960s and 1970s graph theory was used by social scientists to study the behaviour of humans in small groups, resulting in Stanley Milgram's introduction of the notion of the small-world network in his well-known "six degrees of separation" experiment. Graph theory became modern network science in the late 1990s when a number of scientists began to use networks as models of large-scale, real-world phenomena. Newman (2003) is a comprehensive survey of the advances in network theory, and Barabási (2003) is a readable introduction to network science for the general public.

In contemporary scientific research, applications of network science can be found in a wide variety of domains. For example, Newman (2003) surveys work on biological, technological, information, and social networks. However, this may be a modest view. According to the US National Research Council (2005), networks lie at the core of the economic, political, and social fabric of the 21st century. Transportation, power grids, social and economic interaction, business alliances, and military organizations and operations can all be represented in terms of networks and their analytical properties.

It is possible to analyze networks at several levels. At the level of individual nodes and arcs, one may identify measures such as the degree of a node (i.e. how many arcs are linked to it) or its centrality. In a communication network, where arcs represent communication links between C2 nodes, a central position enables fast communications. If a node has a high degree, then it may be classified as a hub in the network. In a social network, the degree measure can be indicative of a person's social status.

At the second level, analysis focuses on clusters of nodes. A cluster in which any one node can send a message to any other is known as a component. Ideally, a complete C2 network should be one giant component, allowing information to flow freely. However, if a C2 network is broken up in several components, the commander's intent will not reach all units, and situation reports from subordinate units may not reach the commander. A C2 network can be broken into multiple components by removing nodes or arcs through equipment failure, enemy action, or lack of interoperability. When targeting a hostile C2 network, one may seek the high-degree hubs, because eliminating these nodes quickly breaks the target networks into separate components. Analysis at the level of clusters can also be used to identify terrorist networks. For example, two clusters representing terrorist cells may be connected by just one node with a high betweenness measure. This node may then represent an information broker or courier between the two cells, making it an attractive target for counter-terrorist operations.

At the level of the network as a whole, one may look at the network's robustness or resilience to failure, at its topology, and at processes occurring through the network. Robustness relates to the number of alternative communication paths through the network. The network topology, whether it is a random graph, a small-world network, or a scale-free (or power-law) network, has an impact on robustness and other network properties. For example, scale-free networks have a hierarchy of hubs, making them vulnerable to targeted attack. Grant, Buizer, and Bertelink (2011) found that representative C2 networks, like the Internet and the World Wide Web, had a scale-free topology. Network processes relating to C2 include the spread of information, epidemiology (i.e. the spread of and recovery from infections), search for information, and network navigation. These processes are influenced by several analytical parameters that may be obtained at the various levels of analysis.

To analyze a network from this multi-level point of view, at least three network metrics are commonly used. The most important metric is the degree distribution of nodes in a network. Degree distribution reveals various properties. At the local atomic level, it may be used to assess whether or not links have been created at random. For example, a power-law degree distribution suggests that the network evolved using a preferential attachment scheme, in which a newly-created node is preferentially linked to a pre-existing, high-degree node, i.e. to a hub. However, as we have seen, such a scheme results in a network that is vulnerable to deliberate attack. Another commonly used metric is the average path length. If the path length is long, communication between nodes that are far apart is at risk of delay and/or failure because of the large number of intermediate nodes that signals must pass through. If path length is low, then nodes are closely tied together, and communication should be faster and less failure-prone. A third metric is the clustering coefficient, related to robustness. This measures the likelihood that two nodes that are linked to a common node, in addition are being linked themselves.

These metrics are also used to characterize and identify three types of network topology. The preferential attachment scheme has already been mentioned, resulting in scale-free networks. Random networks have low average path length and also a low clustering coefficient. Many real-world networks are small worlds, with a low average path length but high clustering.

In management and the military sciences, the concept of networked operations has attained considerable attention. Clearly, there is a dynamic interaction between the various structural properties of networks on the one hand, and new ways of networked operations and supporting technology on the other hand. Therefore, a very important issue is how possible ways of networked operations are affected by the topology and by the architecture of the information, physical and social networks that coexist between various organizational units. Classifying an existing C2 network into one of the three network classes may reveal important strengths, but also weaknesses.

3. APPLICATION TO C2

Around the same time that NEC was being developed in the C2 literature, mathematical network theory began increasingly to yield valuable results. It became clear that these results could be applied equally well to social, information, technological, and biological networks (Newman, 2003). This insight stimulated the thought-leaders to map the NCW / NCO / NEC tenets and value chain into three domains (Alberts, Garstka, Hayes & Signori, 2001). In their view, the *physical domain* represents the real world in which military units manoeuvre, weapon systems engage one another, and sensors capture data about the events taking place. In the information domain, information is created, manipulated, and transmitted, either as spoken or written natural language or as electronic bits and bytes. Invariably, technology is employed to store and transmit information. Traditionally, the technologies used were pen and paper, telephone, and radio, but modern information and communications technologies (ICT) have now surpassed them. Information is received by the human C2 users, converted into knowledge, assessed, and acted upon in the cognitive domain (i.e. in the users' minds). It is in the cognitive domain that C2 decision making – usually modelled by Boyd's (1996) Observe-Orient-Decide-Act (OODA) loop – occurs. Alberts and Hayes (2003) observed that modern military endeavours are too complex to be understood by individuals. Empowered teams working peer-to-peer develop a shared understanding of the situation and of how to respond to this situation. They added a fourth, social domain.

In 2008, Van Ettinger and his NATO colleagues mapped three of the domains (social, cognitive, technical) to networks by means of NATO's (2009) Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability or Information (DOTMLPFI) factors (Van Ettinger, 2008). The technical network covers Materiel (M) and Facilities (F). The cognitive network covers Doctrine (D), Organization (O), and Training (T), and the social network covers Leadership (L) and Personnel (P). In Van Ettinger's depiction, the three networks are shown as overlapping circles, with Interoperability/Information (I) providing the "glue" between them.

By contrast, Monsuur, Grant and Janssen (2011) observed that the three networks were linked by military units and individuals. Being physically embodied, units and individuals appeared as nodes in the technical network. Units and individuals acquired, processed, and acted upon knowledge specific to the application domain. They also appeared, therefore, as nodes in the cognitive network. Since units and individuals communicated with one another, sharing awareness about the situation and synchronizing their actions, they also appeared as nodes in the social network. Monsuur et al termed these interlinking nodes as “actors”, with nodes appearing in only one of the networks being termed “objects”. Since the actors must appear in all three networks, it was easier to depict them as being layered on top of one another. Finally, Monsuur et al’s article provided the basic mathematics for events occurring in one network to influence events in another.

Military interest in the application of modern network science started first and has gained the most intensive form in the United States. In 2003, the US Army proposed that network science should become a new research area. This gained form a year later by the establishment of the Network Science Center (NSC) at the US Military Academy West Point, supported by Dr. David S. Alberts at the US DoD’s Command & Control Research Program (CCRP). The purpose of the NSC is to bring together military officers, civilians, and US Army cadets to research and develop significant contributions in the study of network representations of physical, biological, and social phenomena (NSC, 2014). Interdisciplinary undergraduate courses in network science were developed for the West Point cadets. NSC’s collaborators include US Army research organizations, DARPA, the Naval Postgraduate School, and California State University San Bernardino.

In 2006, the US Army Research Laboratory (ARL) and the UK Ministry of Defence (MoD) formed the Network and Information Science International Technology Alliance (ITA). ITA’s strategic goal is to produce fundamental advances in the information and network sciences that will enhance decision making for coalition operations (ITACS, 2014). The ITA consortium is led by IBM and comprises 24 partners, consisting of eight major defence system integrators and 16 universities, almost equally divided between the US and the UK. In the first phase from 2006 to 2011, ITA adopted four technical areas, one of which was network theory focusing on wireless and sensor networks. The other three areas were not related to network science. In the second phase, due to end in May 2016, ITA has just two technical areas: coalition interoperable secure and hybrid networks, and distributed coalition information processing for decision making. Each area breaks down into three projects, and only the project on the performance of hybrid networks is directly related to network science.

In 2009, the US Army formed the Network Science Collaborative Technology Alliance (NS-CTA), comprising the ARL, CERDEC, and some 30 US industrial R&D laboratories and universities. The goal of the NS-CTA is to develop a deep understanding of the commonalities among intertwined social/cognitive, information, and communication networks, improving the ability to analyze, predict, design, and influence complex systems (NS-CTA, 2014). The CTA’s research program divides into three academic areas focusing on communication, information, and social/cognitive networks. Research is tied together by two cross-cutting issues: trust in distributed decision making, and evolving dynamic integrated networks.

We regard the research done by the USMA’s NSC, the US-UK ITA, and the NS CTA as the representative of the current state of the art.

4. INTERSECTION OF C2 AND NETWORK SCIENCE

4.1 Analysis Framework

To analyze the contributions, we extend the two elements in Lewis' (2009) definition of network science. His definition made a distinction between the theoretical foundations and applications. The same distinction can be made in C2. Since we were seeking contributions that combined network science and C2, our analysis framework is a two-by-two matrix with Lewis' two elements of network science forming the columns and the equivalent two elements of C2 as the rows.

We need to describe each element in more detail. Starting with network science, we can sub-divide the applications according to the domains found in NATO NEC theory: physical, information, cognitive, and social. We modify this scheme slightly in two ways. First, we split off the geographical elements underlying the physical domain into a separate geographical domain. What remains in the physical domain are the objects that can be placed in, or can move around, the geographical domain. This can include roads, buildings, vehicles, sensors, computer hardware, effectors, and other such man-made devices, as well as (groups of) people. Second, the social domain is extended to encompass both informal and formal groups and teams. To recognize this extension, we rename it the socio-organizational domain. Beyond the socio-organizational domain, we identify a coalition level in which multiple organizations (possibly civil as well as military) interact, whether that interaction take the form of deconfliction, coordination, or collaboration.

The theoretical foundations of network science can also be sub-divided. Taking our inspiration from network science surveys, such as Newman (2003), we can distinguish foci of theoretical attention on the properties of nodes and arcs, on network measures such as centrality and betweenness, on network topologies, and on processes occurring in networks, such as search and the spread of information.

Turning now to C2, we can sub-divide the application of C2 according to Boyd's (1996) OODA loop. C2 theory can focus on observation (covering sensing, detection, perception, and monitoring), on orientation (covering the processes needed to understand what has been observed, such as data fusion and intelligence analysis), to decision making, and acting upon these decisions. We note here that action in the C2 context has a strong communicative favour, e.g. sending situation reports and issuing orders. Physical action is largely performed by the resources that are assigned to the commander. Since the OODA loop is reactive in nature, we add the deliberative processes of planning and learning.

To sub-divide the theoretical foundations of C2, we identify a list of issues that recur in the C2 and NEC literature. Starting with individual C2 systems, these issues include providing the underlying infrastructure, gaining and maintaining situation awareness (SA), assessing the quality of information, agility in decision making, and designing a suitable command structure. Then we extend this list by considering issues relating to multiple C2 systems. Issues that arise include interoperability, information sharing, building up a common operational picture (COP), collaboration, self-synchronization, and operational effectiveness (including C2 performance metrics).

In Table 1 we have placed the current state of the art into this analysis framework. The abbreviations NSC, ITA, and CTA refer respectively to the research areas addressed by USMA West Point's Network Science Center, by the US-UK International Technology Alliance, and by the US Army Research Laboratory's Collaborative Technology Alliance. In addition, "Graph" indicates the pre-existing contributions of graph theory to C2 system design, e.g. in calculating the bandwidth available and for frequency management. For example, NSC's mission, as stated on its website, is on the study of network representations of physical, biological, and social phenomena. The publications listed focus on information sharing and on situation understanding (the Orient sub-process in the OODA loop). This has been interpreted in Table 1 as the cells at the intersection of the Information sharing and Orient rows with the physical, information, cognitive, and socio-organizational applications of network science.

Table 1. Mapping the state of the art to analysis framework.

		Network Science									
		Theory:				*Applications:*					
		Nodes	Measure	Topology	Process	Geog	Phy	Info	Cogn	Socio-org	Coalition
C2	*Theory:*										
	Infra	Graph			(Graph)						
	SA										
	Quality										
	Agility										
	Org										
	Interop						ITA	ITA			
	Info sharing						NSC, ITA	NSC	NSC	NSC	
	COP										
	Collab								CTA		
	Self-syn								CTA	CTA	
	Eff'ness										
	Appl:										
	Model										
	Observe						ITA	ITA			
	Orient								NSC, CTA	NSC, CTA	
	Plan										
	Decide										
	Act										
	Learn										

Finally, we sound four cautionary notes. First, other researchers may choose to sub-divide network science and C2 in other ways. Second, our knowledge of the state of the art is based on the information publically available on the organizations' websites. Third, we have not exhaustively reviewed all the relevant literature. We know that there has been surprisingly little about network science in the ICCRTS proceedings from 2005 onwards. Likewise, no books can be found by searching Amazon or Bol.com. However, there may be other conferences and journals – particularly those in network science – where articles on C2 applications may have appeared. Fourth, we have used our judgment in placing the pre-existing state of the art into our analysis framework. This is, of course, necessarily subjective.

4.2 Contributions in Brief

The twelve contributions in the book (Grant, Janssen & Monsuur, 2014) fell naturally into four groups. There were three contributions dealing with organizational issues, another three on how to model C2 networks, four on network theory, and finally two on C2 technology.

The first group consists of the three contributions on organization, command structure, coalitions, and local communities. The first contribution is *De-conflicting Civil-Military Networks* by Van Fenema, Rietjens, and Besters. Using Operation Unified Protector (OUP) in Libya as a case study, they provide insight in suitable network structures and practices for achieving de-confliction between civil and military partner organizations in complex peace operations. They identify several lessons learned, such as coordination depends on the personalities involved, on consistency between rotations, and agreeing on the objectives for the post-conflict environment. They recommend research into reaching agreement on network goals to coordinate civil and military operations. In the second contribution, *Shaping Comprehensive Emergency Response Networks*, Treurniet discusses how professional organizations can incorporate the relevant and useful capacities of local communities in emergency response (ER). He shows how the social capital of communities provide substantial resilience, and contrasts two planning approaches for integrating community capacities into the ER organization. He recommends that ER organizations should strike a balance between directive and empathetic decision making and communication, and identifies the need for further research into effective mixed-sector ER network governance. In the third contribution, *Networked Operations: Taking into Account the Principles of Modular Organizing*, de Waard introduces theory on modular organizing from the organizational and management (O&M) sciences to military forces, contrasting the US and Dutch armies' approaches. He shows that important organizational aspects remain underexposed by only concentrating on the relationship between the number of nodes and network effectiveness, arguing that near-decomposability is an important organizational design parameter. He makes several recommendations for further research, including the need to investigate cycling between centralized and decentralized organizational structures to increase coordination. He advocates applying the O&M debate on subgroup isolation and intergroup connectivity to the military domain, as well as elaborating on the effect of structural holes in organizational networks.

The second group consists of the three contributions on modelling C2. In the fourth contribution, *Modeling Command and Control in Networks*, Jensen proposes an approach to modelling the functions of C2 performed over a network of geographically distributed entities, based on Brehmer's (2007; 2013) C2 theory. Her contribution suggests an approach that enables any C2 organization to be modelled. She recommends the use of empirical data to compare Brehmer's theory with other C2 theories, and the development of sub-theories of the functions of data collection, orientation, and planning. In the fifth contribution, *Formalized Ontology for Representing C2 Systems as Layered Networks*, Grant presents a logical ontology for representing C2 systems from their underlying (cyber-) geography, through physical objects, information, and knowledge, to the socio-organizational constructs. Key contributions include dividing the ontology into layers, integrating cyberspace into the other four "kinetic" domains, and showing that a rich set of C2-relevant networks can be extracted from the ontology. Further research focuses on using the ontology to develop simulation software. In the sixth contribution, *Modeling C2 Networks as Dependencies: Understanding What the Real Issues Are*, Drabble presents a C2 model focusing on capabilities, dependencies, and vulnerabilities. In this model, nodes representing people, groups, resources, locations, and concepts are linked by one or more directed arcs, weighted according to the strength of the inter-node dependency. Implemented systems based on this model allow analysts to rank and identify the most important nodes in a network, their critical vulnerabilities, and their susceptibility to feedback, and to identify the direct, indirect, cascading and cumulative effects of changes in a network. Through an integrated planning capability, analysts can develop plans to alter the behaviour of an opposition network to exploit its vulnerabilities, or to increase the resilience and robustness of their own networks. Drabble recommends the extension of this work to provide the abilities to track plan rationale so that the planner can be re-tasked if an effect can be achieved through a different node, and to update key information as the network changes over time.

The third group consists of the four contributions on network theory. In the seventh contribution, *Dynamical Network Structures in Multi-Layered Networks: Implementing and Evaluating Basic Principles for Collective Behavior*, Janssen, Monsuur, and Van der Wal present a stochastic actor-based method that can be used to analyze the effect of the dynamic behaviour of actors in a network on coordination, synchronization, robustness, and the desired operational effectiveness of a networked organization. They show that, in networked military action, a node is not just part of one network (e.g. a communication network or a social network), but simultaneously belongs to multiple networks. Therefore, to model the dynamical behaviour of actors, one has to take into account the interdependency between networks. They recommend further work in simulating the use of several types of actors, of other measures of performance, and of basic principles other than reciprocity and covering. In the eighth contribution, *Improving C2 Effectiveness Based on Robust Connectivity*, Deller, Tolk, Rabadi, and Bowling, describes an approach to develop an improved metric for network effectiveness through the use of Cares' (2005) Information Age Combat Model (IACM) as a context for combat or competition between networked forces. The value of the Perron-Frobenius Eigenvalue metric, together with a robustness factor, is confirmed using an agent-based simulation, shifting the focus from the capabilities of the nodes to the capability of the network as a whole. Deller et al intend to check whether the results apply to even larger networks. In the ninth contribution, *C2, Networks, and Self-Synchronization*, Dekker explores the connection between C2 and networks to address the question of which network topologies are the best for self-synchronization. He finds by experiment that low average path length, a high node connectivity, and good links between sub-networks all contribute to a network topology suitable for rapid self-synchronization. He recommends that, to avoid group-think, joint, combined, and coalition forces should make networking between components a higher priority than networking within components. Further research is needed to explore new classes of networks (e.g. entangled networks), beyond the well-studied random, scale-free, and small-world models, and to identify which organizational problems benefit best from self-synchronization. In the tenth contribution, *Complex Adaptive Information Networks for Defence: Networks for Self-Synchronization*, Moffat focuses on understanding the nature of the information networks which can create self-synchronization of the force. The analysis is at three levels, covering the basic node and linkage topology (level 1), the local interaction between intelligent nodes sharing information and awareness (level 2), and how such local networking feeds through into emergent clustering effects in the physical domain (level 3). Moffat finds that the tools, modelling approaches, and concepts of complexity theory give a deep insight into self-synchronization.

The fourth and final group consists of the two contributions on C2 technologies. In the eleventh contribution, *Cyber Security in Tactical Network Infrastructure for Command & Control*, Sigholm describes recent developments in emerging network technologies for C2, including reconfigurable radio systems, emerging network topologies, technologies for situational awareness, security metrics, information asset protection systems, and autonomous network monitoring and control. He assesses their maturity using Technology Readiness Levels (TRLs). He concludes that a long-term commitment is required within such areas as procurement, standardization, training, doctrinal and legal development, in order to achieve military utility of C2 systems. He recommends more detailed study of the requirements for tactical C2 network infrastructure to advance these technologies to a TRL that would permit transfer into systems and networks in support of a desired capability, within cost, schedule and risk constraints. In the twelfth and last contribution, *Smart Surveillance Systems*, Rothkrantz argues that, in the near future, the huge amount of heterogeneous, multimodal data received from automated sensor networks will be far beyond the capacity of human operators to fuse, aggregate, and filter. He describes the development of a prototype based on a distributed system of smart agents communicating via blackboards and using Artificial Intelligence techniques such as expert systems, semantic networks, and probabilistic reasoning to give a semantic interpretation of the sensed data. The prototype has been tested using inputs from the Automated Identification System (AIS) monitoring ship movements in and around the Den Helder naval base in the Netherlands. The innovative aspect is the reduction of the role of human operators by using sensors and software agents to observe large areas. He recommends that the current decision support system should be developed as a fully automated system, fusing data from different sources and modalities and integrated with available radar or camera surveillance systems.

4.3 Advances Made

In Table 2 we have placed these contributions into the analysis framework introduced in Section 4.1 above. The numbers in the table's cells refer to the number of the contribution, as follows:

1. Van Fenema, Rietjens, and Besters: *De-conflicting Civil-Military Networks*.
2. Treurniet: *Shaping Comprehensive Emergency Response Networks*.
3. De Waard: *Networked Operations: Taking into Account the Principles of Modular Organizing*.
4. Jensen: *Modeling Command and Control in Networks*.
5. Grant: *Formalized Ontology for Representing C2 Systems as Layered Networks*.

6. Drabble: *Modeling C2 Networks as Dependencies: Understanding What the Real Issues Are*.
7. Janssen, Monsuur, and Van der Wal: *Dynamical Network Structures in Multi-Layered Networks: Implementing and Evaluating Basic Principles for Collective Behavior*.
8. Deller, Tolk, Rabadi, and Bowling: *Improving C2 Effectiveness Based on Robust Connectivity*.
9. Dekker: *C2, Networks, and Self-Synchronization*.
10. Moffat: *Complex Adaptive Information Networks for Defence: Networks for Self-Synchronization*.
11. Sigholm: *Cyber Security in Tactical Network Infrastructure for Command & Control*.
12. Rothkrantz: *Smart Surveillance Systems*.

Table 2. Mapping contributions to analysis framework.

		Network Science									
		Theory:				*Applications:*					
		Nodes	Measure	Topology	Process	Geog	Phy	Info	Cogn	Socio-org	Coalition
C2	*Theory:*										
	Infra	Graph			(Graph)		11	11			
	SA										
	Quality										
	Agility										
	Org									3	2 & 3
	Interop						ITA	ITA			2
	Info sharing						NSC, ITA	NSC	NSC	NSC	2
	COP										2
	Collab							7	CTA	7	2
	Self-syn	10	9				10	7	CTA	CTA + 7	1 & 2
	Eff’ness		8					7		7	
	Appl:										
	Model	5 + 6	6			5	5	5	5	4 + 5	5
	Observe	6	6				ITA + 12	ITA + 12		4	
	Orient	6	6						NSC, CTA	NSC, CTA + 4	
	Plan	6	6							4	
	Decide									4	
	Act									4	

	Learn									4	

It is apparent from Table 2 that the contributions have advanced the state of the art in the literature on the application of network science. In particular, they have addressed a variety of new organizational issues, especially those relating to civil-military interaction (contribution 1), to involving the community in the area of operations (contribution 2), to modular organizations (contribution 3), to modelling C2 (contributions 4, 5, and 6), and to self-synchronization (contributions 9 and 10). Nevertheless, there are many white areas in Table 2, representing areas where future research is needed.

Despite the pre-existing research done by West Point's Network Science Center, the US-UK International Technology Alliance, and ARL's Network Science Collaborative Technology Alliance and the advances reported in the contributions, there are still three main "white areas" in the analysis framework shown in Table 2, as follows:

- The rows corresponding to the application of network science to individual C2 system nodes, covering C2 infrastructure, situation awareness, the quality of information, agility, and the organizational or command structure.
- The columns corresponding to the application of the theory of network topologies and processes into all forms of C2.
- The rows corresponding to the application of network science to C2 decision-making, acting, and learning.

5. CONCLUSIONS AND FURTHER WORK

Network science and network-enabled Command & Control (C2) both emerged in the mid- to late-1990s. However, the two disciplines have developed separately, with separate conferences, journals, and books. Consequently, the authors commissioned a number of scientific contributions to a book aimed at connecting these disciplines (Grant, Janssen & Monsuur, 2014). Researchers from the US, the UK, Australia, Sweden, and the Netherlands provided contributions covering applications ranging from the (cyber-) geography of C2, through physical, technical, information, and cognitive networks, to the socio-organizational level. Case studies ranged from engaging citizens in searching for missing children, through a major fire in a chemical factory and an insurgency scenario, to Operation Unified Protector in Libya and the events of September 11th, 2001.

This paper has placed each contribution into an analysis framework based on the two disciplines' theory and applications. This shows that the contributions form an advance on the current state of the art on the application of network science in C2. In particular, several contributions treat organizations (e.g. military units in a task force) and (civil-military) coalitions as networks. A key limitation is that the current state of the art is assessed on the basis of the publically-stated missions of the Network Science Center, the International Technology Alliance, and the Collaborative Technology Alliance. More exhaustive review and meta-analysis are needed of their publications and of other conferences and journals, particularly in network science.

Despite advancing the state of the art, more research is needed. Each contribution makes its own recommendations for further research. Beyond this, the analysis framework clearly shows “white” areas where little or no work has been done to date: the application of network science to individual C2 system nodes and to decision-making, acting, and learning processes, and the specific application of network topologies and processes to C2 systems. These white areas need to be detailed further by exhaustive review and meta-analysis of the literature.

References

Alberts, D.S. & Hayes, R.E. (1999). *Network Centric Warfare: Developing and leveraging information superiority*. 2nd edition, US DoD Command & Control Research Program, Washington DC, U Washington DC: US DoD Command & Control Research Program.

Alberts, D.S. & Hayes, R.E. (2003). *Power to the Edge: Command Control in the information age*. Washington DC: US DoD Command & Control Research Program.

Alberts, D.S. & Hayes, R.E. (2006). *Understanding Command and Control*. Washington DC: US DoD Command & Control Research Program.

Alberts, D.S. & Hayes, R.E. (2007). *Planning: Complex endeavors*. Washington DC: US DoD Command & Control Research Program.

Alberts, D.S., Garstka, J., Hayes, R.E., & Signori, D.T. (2001). *Understanding Information Age Warfare*. Washington DC: US DoD Command & Control Research Program.

Barabási, A-L. (2003). *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*. New York, NY: Plume.

Brandes, U., Robins, G., McCranie, A. & Wasserman, S. (2013). What is Network Science? *Network Science*, 1 (1), 1-15.

Brehmer, B. (2007). Understanding the Functions of C2 Is the Key to Progress. *The International C2 Journal*, *1*(1), 211-232.

Brehmer, B. (2013). *Insatsledning [Command and control of missions]*.Unpublished technical report, Swedish National Defence College, Stockholm, Sweden.

Boyd, J.R. (1996). *The Essence of Winning and Losing*. Unpublished lecture notes, Maxwell Air Force Base, AL.

Cares, J. (2005). *Distributed Networked Operations: The foundations of Network Centric Warfare*. Newport, RI: Alidade Press.

Cebrowski, A.K., & Garstka, J.H. (1998). Network-Centric Warfare: Its origins and future. In *Proceedings of the US Naval Institute*, 124, 1.

Grant, T.J., Buizer, B.C., & Bertelink, R.J. (2011). Vulnerability of C2 Networks to Attack: Measuring the topology of eleven Dutch Army C2 systems. In Alberts, D.S. (Ed.), *16th International Command & Control Research & Technology Symposium* (paper ID 087), Washington DC: US DoD Command & Control Research Program.

Grant, T.J., Janssen, R.H.M. & Monsuur, H. (2014). Network Topology in Command & Control: Organization, operation, and evolution. IGI Global, Hershey, PA.

ITACS. (2014). US-UK International Technology Alliance Collaboration System. Retrieved February 6, 2014, from https://www.usukita.org/.

JP 1-02. (2013). US Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 as amended through 15 December 2013. Retrieved February 6, 2014, from http://www.dtic.mil/doctrine/dod_dictionary/.

Lewis, T.G. (2009). *Network Science: Theory and applications*. Hoboken, NJ: John Wiley & Sons.

Monsuur, H., Grant, T.J. & Janssen, R.H.P. (2011). Network Topology of Military Command & Control Systems: Where axioms and action meet. In Bauer, J.P. (Ed.), *Computer Science, Technology, and Applications, vol 3* (pp.1-27). Hauppauge, NY: Nova Science Publishers, Inc.

NATO. (2009). *Whitepaper on NNEC Maturity Levels*. Unpublished working draft v2, 22 April 2009. Brussels, Belgium.

National Research Council. (2005). *Network Science: Report of the Committee on Network Science for Future Army Applications*. Washington DC: The National Academies Press.

Newman, M. E. (2003). The Structure and Function of Complex Networks. *SIAM review*, 45(2), 167-256.

NSC. (2014). USMA West Point Network Science Center: about us. Retrieved February 6, 2014, from http://www.westpoint.edu/nsc/SitePages/About.aspx.

NS-CTA. (2014). Network Science Collaborative Technology Alliance, US Army Research Laboratory. Retrieved February 6, 2014, from http://www.ns-cta.org/ns-cta-blog/.

Trist, E. & Bamforth, K. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal Getting. *Human Relations*, 4, 3-38.

Van Ettinger, F. (2008). NATO Network Enabled Capabilities: Can it work? *Carre*, 11, 22-26.