24th International Command and Control Research & Technology Symposium

Topic 2: C2 Concepts

Mission Command when waging cyber operations

Anders Josefsson, Joseph Anderson, Arne Norlander and Björn Marcusson

LtCol Anders Josefsson
E-mail: anders.josefsson@fhs.se
Swedish Defence University, Sweden

LTG (R) Joseph Anderson
E-mail: joea9516@gmail.com
Former Deputy Chief of Staff, G-3/5/7, United States Army

Dr Arne Norlander
E-mail: arne.norlander@gmail.com
Swedish Defence University, Sweden

CDR Björn Marcusson
E-mail: bjorn.marcusson@fhs.se
Swedish Defence University, Sweden

Mission Command when waging cyber operations

Abstract

The conditions for military operations have changed due to many things and the cyber-related challenges associated with these conditions require more attention. Many cyber activities are conducted under other circumstances than conventional war that is called the grey zone between peace and war. The objective of this paper is to explore the conditions for mission command when conducting cyber operations. The distinction between war and peace has blurred and adversaries, both state and non-state, threaten the stability in many western countries. Mission command can be seen both as a philosophy and as a method. The fundamental principles for mission command as a philosophy are trust, intent focus, initiative and common ground. This paper discusses if the conditions for Mission Command have changed and are applicable while conducting different types of cyberspace operations and that offensive and defensive cyber operations imply different conditions for Mission Command. The conclusion is that Mission Command as a philosophy is still relevant, but it has to be supported by a comprehensive Command and Control (C2)-Method that is flexible and able to vary between Direct Control and Mission type Control. The C2 Method should be complemented with a dynamic and adaptive control policy for different types of cyber actions. The paper also suggests a holistic model for Dynamic Command that considers both the situations need for action and the Mission Systems C2-needs.

Keywords: Command and Control, Mission Command, Cyberspace Operations

Introduction

The world is changing and so are the conditions for the execution of military operations. The conditions for C2 of the new ways to execute military operations are also changing. C2 approaches that worked well in the past may not be appropriate today (Alberts, 2018a). If Mission Command was born in high-intensity kinetic warfare there must be a question as to its relevance to a wider spectrum of operations as cyber space operations. The cyber space is a relatively new domain for the operational environment and waging war in that environment has increased the importance of joint operations. Hybrid warfare, and the grey zone between peace and conventional war, gained the western world's attention for more than a decade (Pogoson, 2018; Wirtz, 2017). During the last five years, this concept has been attached to the harmful actions of Russia towards the West (Raitasalo, 2019). Russia might not have been gaining concrete victories during the last years, but has been able to sow chaos and corrode Western societies with its narrative tools in the information and cyber domains (Raitasalo, 2019). Warfare in the grey zone seems to be ongoing all the time and the Western society's armed forces are not designed for waging this kind of war. During the agricultural age usable land constituted people's prosperity and large armies could both take and defend land. After the industrial revolution, there were production nodes and flows of goods that constituted people's prosperity. Long-range fire, impact from aircraft threatened the production nodes and air defense assets protected these nodes. Now we live in the information age where people's prosperity is largely intangible within the cyber domain. In multifunctional and multi-organizational operations, we must have multiple perspectives and an ability to undertake missions in all environments, including the cyberspace domain (Norlander, 2019). The Stuxnet worm that was spread in 2010 marked a watershed in cyberwarfare revealing a level of destructive power with computer code previously reserved for kinetic bombings and physical sabotage (Rosenbaum, 2012). Different types of offensive cyberspace operations threaten the cyber domain and defensive cyberspace operations are the tools to defend against these threats. It is important to develop capabilities for executing cyberspace operations. The problem with commanding cyberspace operations is already recognized one example is formulated by Carvelli (2018), "The United States should delegate cyber-attack authority to operational commanders, but it should impose restrictions on the authority based on the attack's effects". How does this new domain's conditions affect our chosen command philosophy? This paper examines the C2 capability in general and especially for Mission Command in relation to Cyberspace Operations.

The question this paper will try to answer is whether Mission Command is appropriate for cyberspace operations. The objective of this paper is to explore the conditions for Mission Command when conducting cyberspace operations.

To be able to answer the research question, the paper develops a model for analysis of C2 in different situations and with different mission systems.

Mission Command

Mission Command is an English translation of German *Auftragstaktik*. The roots of Auftragtaktik comes from the ideas of the Age of Enlightment and German Romanticism, in the late 1700s and early 1800s, about the individual as a free and independent citizen (Mattsson, 2003).

> *Der Mensh ist das einzige Geschöpf, das erzogen warden muss. Unter der Erziehung nämlich verstehen wir die Wartung (Verpflegung, Unterhaltung), Disziplin (Zucht) und Unterweisung nebst der Bildung*[1] (Kant, 1803).

This meant that soldiers and officers were seen as active creative individuals with their own initiative and will. Mission Command origins for military use can be traced at least as far back as the Napoleonic Wars, after the disastrous defeat of the Prussians at Jena and Auerstedt in 1806 (Widder, 2002). Napoleon's modern brand of warfare exposed Prussian deficiencies and the need for modernizing the Prussian Army. Initial reform was brought about by the infantry drill regulations of 1812, in which the set-piece conduct of battle was abolished, and at least for the higher levels of command, initiative and independent thought and action became important factors.

Mission Command is of great importance for today's leaders and its importance for most of Western society's armed forces ways of leading is described over the years in several of the countries doctrines. Mission Command is also referred to as a key factor enabling Maneuver Warfare (Lind, 1985). In various doctrines, however, different definitions of the term Mission Command are used. Different doctrines also differ concerning the view of whether Mission Command is a philosophy or a method.

To be able to define Mission Command we must first decouple Command from Control for the term Command and Control (C2) as was suggested by Pigeau & McCann (2002) and later by Teske, et al, (2018). The big difference between Command and Control rests on two fundamentally important and uniquely human characteristics: creativity and will (Pigeau & McCann, 2002). The research in this paper is based on the assumption that only humans Command. We use the definition, of Command, suggested by Pigeau & McCann: "*the creative expression of human will necessary to accomplish the mission*" (Pigeau & McCann, 2002). We believe that creativity is one of the most important requirements for Command.[2] Control in the cybernetic sense involves a feedback mechanism by which the real outcome is compared with the formulated goal: action is then taken that minimizes the difference between the two[3]. However, Control in military operations implies more than simply feedback mechanisms. It implies the personnel, facilities and procedures for planning, directing and coordinating resources in the accomplishment of the mission (Pigeau & McCann, 2002). Thus, we use the definition of Control suggested by Pigeau & McCann: "*the act of enabling command and of managing risk using existing structures and processes*" (Pigeau & McCann, 2002).

Because we assume that Command is performed by humans, we choose to study Mission Command where we separate it as a philosophy from Mission Command as a method because a method is more linked to Control with dependencies on organizational structures, processes, technology, etc.

Mission Command as a Philosophy

In general, a philosophy describes a way of thinking, in other words, "a system of faith that affects someone's decision and behavior" (Macmillan Dictionary).

---

[1] Author's translation: *Man is the only creature to be educated. Under education, we understand the maintenance (food, care), discipline and instruction along with the education*.

[2] S.L.A. Marshall (1947) suggested that "60 percent of the art of command is the ability to anticipate; 40 percent is the ability to improvise, to reject the preconceived idea that has been tested and proved wrong in the crucible of operations and to rule by action instead of acting by rules." (p.108.)

[3] See Weiner, N. (1961) for a fuller treatment.

The philosophical perspective on Mission Command focuses on human relations and emphasizes that subordinate commanders are qualified to make decisions and take initiative (Granåsen, et al, 2018). Mission Command as a philosophy, is also laid at the view on the nature of war and the principle of dual responsibility. A German article in *Militär-Wochenblatt* from 1906 puts it this way:

> *We [the German Army] have no use for soldiers without a will of their own who will obey their leaders unconditionally. We need self-confident men [and women] who use their whole intelligence and personality on behalf of the senior commander's intent* (van den Bergh, 1906).

Mission Command is fundamentally a decentralized style of Command, a philosophy of decentralized Command relying on initiative, acceptance of responsibility and mutual trust (Storr, 2003). Responsibility for superiors and subordinates involves an altruistic attitude in the individual's actions.

A fact that points out that Mission Command is about so much more than giving orders in the form of a mission is that it is clearly emphasized that the mission must be reconsidered if it was not found appropriate.

> *The mission and the situation are the basis of command. The mission refers to the objective to be pursued. It must not fall out of sight at the Commander. Uncertainty about the situation is the rule. From the mission and the situation comes the decision. When the mission no longer suffices as the basis for the action and has become obsolete by the changed situation, the decision must consider these circumstances. (Heerensdienstvorschrift, 1933).*

The effective application of Mission Command is dependent on individual willingness and capability to apply non-conformist and unique solutions when crises arises. The readiness of all ranks to depart from "the plan" once it no longer supports the Commander´s desired End State is essential and must be assumable by each level of Command (O´Leary, 1999).

Barius (2012) identifies four fundamental principles that need to be in place to apply Mission Command - Trust, Intent focus, Initiative and Common Ground. Flynn & Schrankel (2013) similarly identify five factors: Trust, Intent, Initiative, Mission Order and Risk Acceptance. Based on the above description and the factors developed by Barius 2012 and Flynn & Schrankel 2013, this paper uses the following factors: *trust, intent, initiative* and *common base* as essential elements to be able to employ Mission Command.

Trust between commanders and their subordinates is essential for effective Command as a large portion of the execution of operations is handed over to subordinate commanders (Granåsen, et al, 2018).

Intent focused means clarifing *what* has to be achieved and hand over the *how* part to subordinates, allowing freedom of action and robustness to subordinate levels as the situation changes (Flynn & Schrankel, 2013; Finkel, 2011).

Initiative means that there needs to be a willingness to take initiative throughout the organization and to exploit opportunities as they arise (Flynn & Schrankel, 2013).

Common ground means that people in the organization have common values and common understanding of the doctrine, which creates a mutual cognitive understanding; this creates an environment that enables commanders to delegate *how* the objective should be reached (Barius, 2012).

Mission Command as a Methodology

A method is a way of doing something, especially a planned or established way, "methods that you use to do something are like tools and machines" (Macmillan Dictionary).

The method perspective on Mission Command can be seen as a part of control structures and processes, which are human inventions to support command. The method for Mission Command means that commanders give mission orders with objectives and guidelines, while subordinate commanders receive extensive independence, this enables flexibility and adaptation of the dynamic battlefield. Applying Mission Command as a method should enable faster decision-making in relation to the opponent and thus make his countermeasures ineffective (Brehmer, 2005).

The method for conducting Mission Command can be manifested in the build up of mission orders. Commanders use mission orders to assign tasks, allocate resources, and issue broad guidance (US Army, 2012). The factors for using a method for Mission Command can be specified as:

- Give Mission orders:
    - Specify the goals to be achieved and for what purpose (*why*).
    - Give broad tasks (*what*).
    - Assign resources to solve the tasks.
    - Give only necessary rules of engagement.
- Submit as much as possible to subordinates to decide for themselves how the mission should be accomplished (*how*).

The above described method supports Mission Command as a philosophy because it reinforces the belief in man and thus provides a good basis for mutual trust.

Cyberspace operations

The key elements of cyberspace operations have their parallels to operations in other domains such as land, sea, air or space. No matter what type of military operation we are aiming for, it must be linked to a political goal (Singer, 2014). Most aspects of joint operations rely in part on cyberspace, which is the domain within the information environment that consists of the interdependent network of information technology infrastructures and resident data (Joint Chiefs of Staff, 2018).

Several definitions of cyberspace can be found both in scientific literature and in governmental sources. Cyberspace consists of myriad different and often overlapping elements to include networks, nodes, links, interrelated applications, user data, and system data (Ibid). In this paper we use the definition of cyberspace used in Department of Defense Joint Terminology for cyberspace: "*Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures*" (DoD, 2010).

Cyberspace Operations (CO) can be defined in many ways. In this paper, we use the definition presented in United States Joint Publication 3-12: "*CO is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace*" (Joint Chiefs of Staff, 2018).

The bottom line of what distinguishes CO from other military operations is its digital means and digital targets (Singer, 2014). This means that the cyber domain and the digital landscape can be completely changed by updating e.g. software, which does not apply to the other domains

of the operating environment. From that statement we can find specific conditions for C2 that emerges from CO.

Alberts (2018b) states that Cyberspace Operations require a non-traditional C2 approach and that not all Cyberspace Operations are the same. There are differences between defensive Cyberspace Operations that seek to defend and thus assure the performance of cyberspace assets and capabilities and those that are offensive in nature (Alberts, 2018b).

There are two primary types of CO:

- Offensive Cyberspace Operations (OCO)
- Defensive Cyberspace Operations (DCO)

OCO are intended to project power in and through foreign cyberspace through actions taken in support of national objectives (Joint Chiefs of Staff, 2018). What distinguishes an OCO from other types of military operations? To begin, OCO employ different means. Instead of using kinetic force like bullets or bombs, OCO use digital means, computer actions of some sort (Singer, 2014). Thus, OCO is not constrained by the usual physics of traditional operations. In cyberspace attacks can literally move at the speed of light, unlimited by geography and political borders. The second way OCO differs is in the target. Instead of causing direct physical damage, OCO first targets another computer and the information within it (Ibid). The intended results may be to damage something physical, but that damage always first results from an incident in the cyber domain. OCO may exclusively target adversary cyberspace functions or create first-order effects in cyberspace to initiate cascading effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, high-value targets, etc. (Joint Chiefs of Staff, 2018).

DCO are executed to defend own governmental cyberspace resources, or other cyberspace defense forces that have been ordered to defend from active threats in cyberspace. Specifically, they are intended to preserve the ability to utilize own cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity (Joint Chiefs of Staff, 2018).

Holistic Model for Dynamic Command

This paper proposes a model for exploring a suitable scope of various missions. It's called a Holistic Model for Dynamic Command. The model is designed for the analysis to be able to take into account both the situation that is to be influenced and the various functions that constitutes the mission system that executes the actions to affect the situation.

In this paper we choose to the view the world from a system perspective and there are several ways to represent systems in form of models, which can be seen as abstract representations of real or virtual phenomena (Buede & Miller, 2016).

We assume that C2 influences the Situation System through a Mission System which can be seen as an interface between the two (figure 1), as described in a paper from 23rd ICCRTS (Hallberg, et al, 2018).

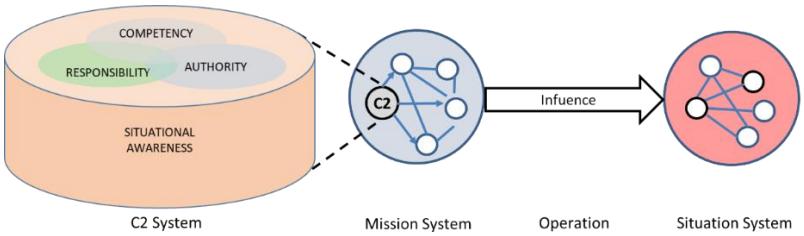

Figure 1 Holistic Model for Dynamic Command in a systems perspective

The Situation System in figure 1 is a description of the situation and contains unacceptable conditions that have to be changed to acceptable conditions. The creation of effects that supports the Situation System transition from an unacceptable to an acceptable condition is done by an operation which is conducted by the Mission System in figure 1. Thus, the Mission System have to be designed to meet the needs for actions that creates desired effects in the Situation System. Likewise the C2 System, in figure 1, should be designed to meet the C2 needs and produce what Ashby (1963) called the "requisite variety" to match the Mission System. The degree of centralization is dependent on the level of detail required in the directives issued by headquarters for each type of Mission System (Alberts, et al, 2001). We believe that we have to take the Mission Systems functions into account when analyzing a C2 philosophy (or method) that shall direct the Mission System in order to achieve effects in the Situation System.

In this paper we use the Holistic Model for Dynamic Command in a systems perspective where the four dimensions of command capability (competency, situation awareness, authority and responsibility) are studied for a specific Mission System that conducts cyberspace operations to change unacceptable conditions in the Situation System.

Situation System

The description of the Situation System's characteristics are influenced by the suggestion for Endeavour Space Dimensions by Johansson, Carlerby & Alberts (2018): coupling/causality, dynamics and degree of complexity/tractability. In this paper we separate coupling from causality and complexity from tractability. In addition, we propose two characteristics to make the description of the situation more complete. The first of these two new factors is *impactability*, which is needed to understand how easy or difficult it is to influence the situation. The second of these two new factors is *time conctraints*, which is needed to understand how quickly the situation needs to be affected so that it does not escalate and becomes too difficult to handle.

This paper suggests thus that a *Situation Systems* characteristic can be divided in to the following general categories:

- *Impactability* (how easy the situation system can be affected or influenced).
- *Coupling* (number of relationships between the elements of the situation).
- *Causality* (how easy is it to predict causal relationships).
- *Traceability* (how easy it is to subsequently understand the causes of what happens).
- *Dynamics* (how many changes in the situation take place while the situation is going on).
- *Time constraints* (how urgent it is to solve the situation and how long the situation is assessed to continue).

For each characteristic, we use the low - medium - high scale to assess the Situation System. The indicators we have used for classifying the characteristic are described in the analysis.

Mission System

Both the operations characteristic and the capabilities of the Mission System are of course important building blocks to understand the need for C2. In this paper we suggest that analysis of the Mission System as a baseline uses six types of operational functions[4] (for analysis of each operational function we use questions that support the analysis):

- *Effects functions* that are needed to fulfill the purpose of the organization. The effects functions differ from organization to organization. A military organization have maneuver to gain positional advantage in respect to the adversary, fire and information to create an effect on the target to accomplish the mission.[5] A hospital can have life saving and health care as effect functions. What resources can reach the target? How far can the resources have effect? How fast can the resources act?
- *C2 function* provides direction and coordination to the military effort in order to produce military effects (Brehmer, 2007). Who can coordinate the resources when executing the planned action? Time for planning?
- *Intelligence function* to contribute to a continuous and coordinated understanding of the situation. Who can see the target? Who can analyze the target? Time to support decision making?
- *Sustainment function* to maintain freedom of action and capability throughout the whole operation.
- *Protection function* to protect friendly forces in order to minimize the vulnerability of these forces to preserve freedom of action.
- *Collaboration function* that enables a broad spectrum of interaction with other actors.

C2 System Model

The C2 System Model is developed based on results in a paper from 23rd ICCRTS (Hallberg, et al, 2018). This paper suggests that the C2 System Model can be represented in four different views depending on what you want to represent:

- *Conditional view* that describes conditions that have to be in place to be able to perform efficient command (will be described in detail below)
- *C2 functions view* that shows the general C2 functions that are needed to provide the purpose of C2, namely direction and coordination, these functions are: Data providing, Orienting (Assessing & Estimating), Planning, Influencing and Communicating (will not be further used in this paper for assessing Mission Command in Cyberspace Operations).
- *Systems Elements view* that describes the form of the system elements in the C2 system namely: doctrine, method, organization, personnel and technology (will not be further used in this paper for assessing Mission Command in Cyberspace Operations).
- *C2 products view* that shows the products produced by the C2 functions: situation picture produced by data providing function, implication of the situation produced by

[4] The operational functions are inspired by Nato joint functions (Nato, 2019) and US Army's warfighting functions (US Army, 2017)

[5] The effects function can be seen as a merger of Nato joint functions manoeuvre, fires and information (Nato, 2019).

the assessing function, intent produced by the estimating function, plan produced by the planning function, order produced by the influencing function and transferred message produced by the communicating function (will not be further used in this paper for assessing Mission Command in Cyberspace Operations).

The conditional view of the C2 System Model is founded on original work by Pigeau & McCann (2001), and is further developed by Norlander (2011).

The conditional view considers four conditions that have to be in place to achieve Command Capability: competency, situation awareness, authority and responsibility.

Competency
Commanders at all command echelons need skills and abilities for accomplishing missions.

Physical competency includes physical strength to fulfill the mission but also sophisticated sensory motor skills, good health agility and endurance.

Intellectual competency includes using reasoning, critical thinking, creativity, flexibility, ability to constructive thinking and willingness to learn.

Emotional competency includes resilience, hardiness and the ability to cope under stress. The ability to keep an overall emotional balance and perspective on the situation is critical.

Interpersonal competency is essential for interacting effectively with subordinates, peers, superiors, the media and other government organizations. It includes social skill with attributes of trust, respect, perceptiveness and empathy.

Situation Awareness
To be able to make decisions in certain situations, within an operational environment, commanders need Situation Awareness (SA). SA is basically knowing what is going on around you (Endsley, 1995) which means that the decision maker has to be able to see the target. We mean that SA also means that the decision maker must understand the effects and consequences of actions that are to be decided. As Brehmer (2006) puts it “the decision maker must reach action oriented understanding” (Brehmer, 2006).

Authority
Authority is the degree to which a commander is empowered to act. There is a distinction between the legal authority that is assigned from superior command and personal authority which is what individuals earns by virtue of personal credibility.

Responsibility
Responsibility addresses the degree to which an individual accepts the legal and moral liability commensurate with command. As with authority, there are two components to responsibility, one externally imposed and the other internally generated. The first, called extrinsic responsibility, involves the obligation for public accountability. Extrinsic responsibility is the degree to which an individual feels accountable both up to superiors and down to subordinates.

The second called intrinsic responsibility is the degree of self-generated obligation that one feels towards the military mission. It is a function of the resolve and motivation that an individual brings to a problem — the amount of ownership taken and the amount of commitment expressed.

The Recursive perspective of the holistic model for dynamic command

Stafford Beer (1981) provides a recursive model called the Viable Systems Model (VSM) based on cybernetic principles and organization theory. VSM represent a system of systems perspective in different levels of Command and has a Control component on each level. In this paper we have to use a model that describes both C2 systems and Mission Systems at different echelons of Command to be able to study the relevance of Mission Command. We base our work on a model founded in a paper from 23rd ICCRTS (Hallberg, et al, 2018).

The recursive perspective in figure 2, focuses on the fact that Command and C2 systems are used in a hierarchy with several echelons of Command within the Armed Forces.

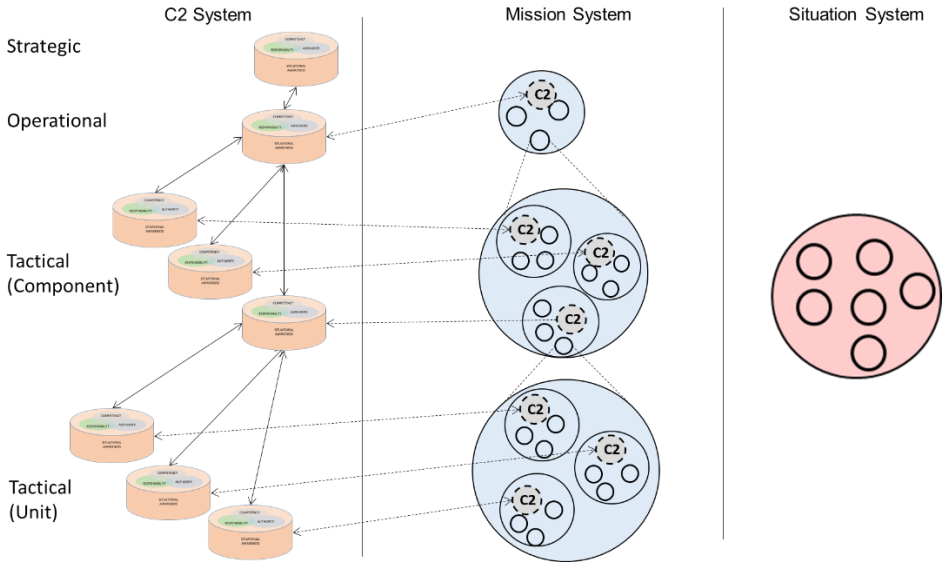

Figure 2 Model for dynamic command in a systems perspective

It is normally on the units' level in this system of systems model (figure 2) that the interaction occurs with the Situation System where the desired effects are to be created. In this paper, we use the conditional view for each echelon of Command to consider under which echelon the Command of cyberspace operations are best suited.

Analysis of Mission Command in Cyberspace Operations

We use the holistic model for dynamic command and analyze how both the factors for Mission Command as a philosophy are met and how the factors for Mission Command as a method are met when conducting both OCO and DCO. We will use two cases to study whether Mission Command is appropriate for Cyberspace Operations. The cases are: Stuxnet and Maersk. We choose these two cases because they are well known and there is a lot of documentation about them. In addition, they have been executed by different actors and by different methods.

Case Stuxnet

Stuxnet marked a watershed in cyberwarfare, not only demonstrating United States of America´s willingness to engage in offensive cyberattacks against its most intransigent adversaries, but also revealing a level of destructive power with computer code previously reserved for kinetic bombings and physical sabotage (Rosenbaum, 2012). The purpose of Stuxnet and other acts of cyberwarfare is inherently political. Stuxnet is a sophisticated worm designed to target specific Supervisory Control And Data Acquisition (SCADA) systems produced by Siemens. SCADA-systems are used for industrial control. The Stuxnet Worm first

emerged during the summer of 2010 and was a computer worm that infiltrated numerous computer systems (Broad, 2011). Stuxnet launched a series of attacks targeting industrial controllers used at Iran's uranium enrichment facility in Natanz (Williams, 2016). Industrial controllers are small computer systems that run mechanical devices such as pumps, valves, motors, and thermometers by sending and receiving electrical signals (Lagner, 2011). First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself as it infected system after system. From there it sought
out Siemens Step7 software, which is also a Windows-based system used to program industrial controllers that operate equipment, such as centrifuges. The industrial controllers were not connected to the internet at all (Knapp et. al., 2015). Over fifteen Iranian facilities were attacked and infiltrated by the Stuxnet worm. One of the affected industrial facilities was the Natanz nuclear facility. The Institute for Science and International Security (ISIS) suggest, in a report published in December 2010 that Stuxnet is a reasonable explanation for the apparent damage at Natanz and may have destroyed up to 1,000 centrifuges (10 percent) sometime between November 2009 and late January 2010 (Albright et. al., 2010). It is believed that this attack was initiated by a random worker's USB drive (Broad, 2011). The attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. If its goal was to quickly destroy all the centrifuges in the Fuel Enrichment Plant [FEP], Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily (Albright, et al, 2010). Each time Stuxnet infected a system, it "phoned home" to report information about the infected machines (Ibid). After Stuxnet's discovery, Iran accused NATO and the US of involvement in the attacks, but both have denied responsibility. Some have also suspected Israel's Unit 8200 security agency. Israel hasn't publicly commented on Stuxnet but acknowledges that cyberwarfare is now part of its mission (Chen, 2011).

Situation System

The Situation System (SS) for the OCO was Iran's nuclear program and it's FEP. The assessment of SS characteristic are:

- The *impactability* was ***low*** and it was not easy to influence since the FEP with its industrial controllers was not connected to the internet.
- The *coupling* between the elements in the situation can be considered as ***medium*** since the first target was coupled to the second target which was the industrial controllers controlling the centrifuges in the FEP. The number of relations between the elements can however be considered as ***low***.
- The *causality* was ***medium*** since there had been a lot of research on the Stuxnet functionality and good intelligence on SS construction.
- The *traceability* can be considered as ***medium*** since the Stuxnet "phoned" home to report information about the infected systems.
- The *dynamics* in the SS can be considered as ***low*** since there was no AI involved in this kind of industrial system. Which meant that the system itself could not impart any real dynamics but only human operators.
- The *time constraints* are assessed as ***low*** since the time for planning and execution was on the attacker's side.

The SS for the DCO are FEP that start to behave strange when attacked by Stuxnet worms and the characteristics are:

- The *impactability* of the Stuxnet worm can be considered as ***low*** since the defender did not have a clue what caused the change in the centrifuge's rotor speed.
- The *coupling* between elements in the situation can be considered as ***high*** since Stuxnet was developed in several steps, which made it difficult for the defender.
- The *causality* can be considered as **low** since we assess that it was difficult for the defender to foresee what to do to stop the attack
- The *traceability* can be considered as ***low*** since it was hard for the defender to trace the causes of why the centrifuges rotor speed changed.
- The *dynamics* can be considered as ***high*** since the Stuxnet first raised the speed of the centrifuges and then lowered it.
- The *time constraints* are assessed as ***high*** since the defender had short time to protect its FEP before it would break down.

In the Stuxnet case, we can see that the situation implies very different conditions for the actor who executes the OCO and the actor executing the DCO. The first important difference are *dynamics* that can be considered as low for OCO while it is assessed as high for DCO. The second important difference is time constraints that also can be considered as low for OCO while it's assessed as high for DCO.

Mission System
The assessment of Mission System (MS) for the OCO are:

- The *Effects function* that created effects on the target was provided by agents who infiltrated the USB Drive loaded with the Stuxnet worm and data hackers in other countries who controlled the the behavior of the Stuxnet worm. The Stuxnet worm had effects at ***very long distance*** with ***high speed*** after it had been injected.
- The *C2 function* was most likely provided by ***central coordination*** of the attack after a ***long planning time***.
- The *Intelligence function* was probably provided by ***many different intelligence resources that could see the target*** in some way and research teams that gained knowledge of how the industrial controllers of the FEP worked. The intelligence function had a ***long time to analyze*** data to support decision making.
- The *Sustainment function* was probably provided by many teams in many ***different locations*** to both sustain the operation.
- The *Protection function* was probably also provided by many teams in many ***different locations*** to protect the operation.
- The *Collaboration function* was likely needed to enable a lot of interaction with ***many different actors*** outside the actual mission system.

The assessment of Mission System (MS) for the DCO are:

- The *Effects function* that tried to stop the effects from the Stuxnet worm were most likely initially provided by already installed firewalls and ***local technicians***.
- The *C2 function* was most likely initially provided by ***local site managers***, with almost no time for planning, and later by central management for the whole nuclear program.
- The *Intelligence function* was probably immediately provided by ***local technicians*** with a very short time to support decision making. Later it probably was provided by Iran's national intelligence resources when it was too late to support decision making to stop the attack.
- The *Sustainment function* was most likely initially provided by ***local teams*** at the FEP.

- The *Protection function* was most probably initialy provided by local teams at the spot of the attack.
- The *Collaboration function* was likely initiated quite late when local managers understood that they needed help from others.

In the Stuxnet case we can see many differences between the Mission System used in OCO and DCO. The effects function had effect globally for the OCO and locally for the DCO. The C2 function was provided by central command with long planning time for the OCO while it was provided by local managers with no time for planning for the DCO. The intelligence function for the OCO could see the target in some way from a very long distance while the DCO only had local and poor intelligence when it was time to support the manager's decision making. Both the sustainment and the protection function for OCO was globally while it initially was local for the DCO. The collaboration function for OCO was developed under a long time and with many actors outside the mission system while collaboration, initially after the attack, was performed locally for the DCO.

C2 System
The conditional view of the C2 System for OCO:

- *Competency* for command is assessed to be ***best at higher echelons*** since the operation needed lot of coordination of all operational functions within the mission system and thus the commander needed support from a HQ with many different skills.
- *Situational awareness* for command is assessed to ***be best at higher echelons*** since the higher echelons can have intelligence from many sources in different places and also has the best conditions to understand the second degree effects and consequences
- *Authority* for command is assessed to be ***best at a very high echelon*** both because the attack could have major strategic consequences and that many parts of the operation needed to be coordinated.
- *Responsibility* for command is assessed to be best at ***higher echelons*** as it is most likely that both extrinsic responsibility and intrinsic responsibility is obtained when the commander works close to the political level and really understands the purpose of why the operation is carried out.

The conditional view of the C2 System for DCO:

- *Competency* for command is assessed to be ***best at lower echelons*** since the impact of the OCO means that the local manager who is commanding DCO needs both a lot of intellectual competency to understand what is happening and a lot interpersonal competence to execute the local manager's decisions.
- *Situational awareness* for command is assessed to be ***best at lower echelons*** since it is local that the symptoms are first detected and the direct implication can be quickly understood.
- *Authority* for command are assessed to be ***best at the lowest echelon*** because the time to decide on countermeasures is extremely short.
- *Responsibility* for command is assessed to be ***best at lower echelons*** as they are judged to have great responsibility for a functioning facility and for their staff to contribute to this process.

In the Stuxnet case, we can see that everything differs between OCO and DCO regarding conditions for command. Conditions to meet the C2 needs when executing an OCO are clearly best at higher echelon and equally clearly best at lower echelon when executing a DCO.

Case Maersk

The attack at Maersk by a NotPetya Virus on June 27, 2017, started as an attack on the Ukrainian government and business computer systems to disrupt that country's financial system (Perlroth, 2017). Supposed Russian hackers hijacked the Linkos Group, a small, family-run Ukrainian software business and their update servers that pushed out infected updates into thousands of PCs around the country through a hidden back door (Greenberg, 2018). The update servers used a software called M.E.Doc, which is used by nearly anyone who files taxes or does business in the country (Ibid). The hackers used M.E.Doc to push out infected code to spread automatically, rapidly, and indiscriminately. In this case we could see massive cascading effects. Port operations were suspended in several port terminals controlled by Maersk division, in the United States, India, Spain, the Netherlands and other countries (Silgado, 2018). The users of the computers all around the world could read "repairing file system on C:" with a warning to turn of the computer (Greenberg, 2018). Within half an hour the full scale of the crises became clear to Maersk management and disconnecting Maersk's entire global network took approximately two hours (Ibid). That meant no containers were received or delivered in 76 Maersk Ports, resulting in significant business interruption during the shutdown period (Novet, 2017). The impact of the cyber-attack was around USD 300-400 million in lost revenue, 45.000 computers affected, and the paralysis of cargo transport through the company's ships and ports (Silgado, 2018).

Situation System

The SS for the OCO was the Ukrainian financial system. The assessment of SS characteristic are:

- The *impactability* was ***high*** as the SS was connected to the internet and used ordinary Windows software.
- The *coupling* between the elements in the situation can be considered as ***high*** as servers automatically pushed out infected code to many PCs using M.E.Doc for taxes and business.
- The *causality* can be considered as ***medium*** since a lot of research on the NotPetya's functionality had been done but the attacker couldn't know which computers would be infected and thus not know the secondary effects.
- The *traceability* can be considered as ***low*** since it was not possible to follow the path of the infected code.
- The *dynamics* in the SS can be considered as ***low*** since the update servers were programmed to automatically send out updates.
- The *time constraints* are assessed as ***low*** since the time for planning and execution was on the attacker's side.

The SS for the DCO are PCs at many different places all around the world that stop functioning when attacked by NotPetya Virus and the SS characteristics are:

- The *impactability* of the NotPetya Virus can be considered as ***low*** since the defender did not know why their PCs stopped functioning.
- The *coupling* between SS elements are assessed as ***high*** since the infected code on the local PCs was automatically pushed out from update servers.
- The *causality* can be considered as **low** since we assess that it was difficult for the defender to foresee what to do to stop the attack.
- The *traceability* can be considered as ***low*** since it was hard for the defender to trace the causes that their PCs had black screens.

- The *dynamics* can be considered as ***low*** since the PCs had black screens with messages saying "repairing file system on C:".
- The *time constraints* are assessed as ***high*** since the defender had a short time to fix the computers so their business could be controlled safely.

In the Maersk case, we can see that the situation also implies very different conditions for the actor who executes the OCO and the actor executing the DCO. The first important difference is *impactability* on the SS that can be considered as high for OCO while it is assessed as low for DCO. The second important difference is time constraints that also can be considered as low for OCO while it is assessed as high for DCO.

Mission System
The assessment of MS for the OCO are:

- The *Effects function* that created effects on the target was provided by hackers that infected update servers with NotPetya Virus via the internet. The NotPetya Virus had effect over a ***very long distance*** with ***high speed***.
- The *C2 function* was most likely provided by ***central direction*** of the attack after a ***long planning time***.
- The *Intelligence function* was probably provided by ***the hackers*** that gained knowledge of how the Ukrainian financial system used their computers and software. The intelligence function had a ***long time to analyze*** data to support their decision making.
- The *Sustainment function* was probably not very large since it was small units of hackers who needed to be sustained during the operation.
- The *Protection function* was probably not very large since it was small units of hackers, on a long distance from the target, needed needed to be protected during the operation.
- The *Collaboration function* was likely ***not used much*** in this operation since there were not many actors outside the actual mission system.

The assessment of MS for the DCO are:

- The *Effects function* that tried to stop the effects from the NotPetya Virus were most likely initially provided by already installed firewalls and ***local technicians*** quite soon.
- The *C2 function* was most likely initially provided by ***local site managers***, with almost no time for planning, and within half an hour by central management at Maersk and other infected actors.
- The *Intelligence function* was probably immediately provided by ***local technicians*** in a very short time to support decision making and in half an hour provided by the Maersk ***central management team***. Later many nations' national intelligence resources probably provided intelligence when it was too late to support decision making to stop the attack.
- The *Sustainment function* was most likely initially provided by ***local teams*** and later by Maersk's ***whole logistic resourses***.
- The *Protection function* was most likely initially provided by ***small local teams*** that later was reinforced by contractors.
- The internal *Collaboration function* within Maersk and other affected actors was likely ***initiated almost immediately*** while external collaboration probably took longer.

In the Maersk case we can see many differences between the Mission System used in OCO and DCO. The effects function had global impact immediately for the OCO and first locally then

globally within two hours for the DCO. The C2 function was provided by central command with a long planning time for the OCO while the DCO C2 first was provided by local managers with no time for planning and within half an hour by central managers who had enormous time constraints. The intelligence function for the OCO could see the target in some way from a very long distance while the DCO first had local and poor intelligence and within half an hour global but equally poor intelligence. The sustainment function for OCO didn't have to be so extensive while it quickly went from local to central for the DCO. The protection function was most likely small for both OCO and DCO. The collaboration function for OCO was probably not used much while it was extensive internally for the DCO.

C2 System

The conditional view of the C2 System for OCO:

- *Competency* for command is considered to be ***best at higher echelons*** since it require wise judgment to decide on OCO.
- *Situational awareness* for command is assessed to ***be best at higher echelons*** since higher echelons can have intelligence from many sources in different places and also has the best conditions to understand the second degree effects and consequences
- *Authority* for command is assessed to be ***best at a very high echelon*** both because the attack could have major strategic consequences and that many parts of the operation needed to be coordinated.
- *Responsibility* for command is assessed to be best at ***higher echelons*** as it is most likely that both extrinsic responsibility and intrinsic responsibility are obtained when the commanders work close with the political level and really understand the purpose of why the operation is carried out.

The conditional view of the C2 System for DCO:

- *Competency* for command is assessed to be ***best at lower echelons*** since the impact of the OCO means that the local manager who is commanding DCO needs both a lot of intellectual competency to understand what's happening and a lot interpersonal competency to execute the local manager's decisions.
- *Situational awareness* for command is assessed to ***first*** be ***best at lower echelons*** since it is local where the symptoms are first detected and the direct implication can be quickly understood. ***After the data is reported, compiled and assessed the higher echelons probably have better situational awareness***.
- *Authority* for command is assessed to ***first*** be ***best at the lowest echelon*** because the time to decide on countermeasures is extremely short. For decisions with ***global impact*** the authority, needs to be moved to ***higher command***.
- *Responsibility* for command is assessed to be ***best at lower echelons*** as they are judged to have great responsibility for their local business. When it comes to decisions with global impact the responsibility is considered to be ***best at higher echelons***.

In the Maersk case, we can see that almost everything differs between OCO and DCO regarding conditions for command. Conditions to lead OCO are clearly best at higher echelon but when it comes to DCO the conditions change over time. When an organization is influenced by a cyber-attack, the conditions for command are immediately better at lower echelons while conditions for making decisions with global impact for the organization are better at higher echelons.

From both case studies we generally have observed that OCO has the following characteristics: O1 Long time for planning; O2 Use of digital means (computers); O3 Attacks can move at the speed of light; O4 Absence of geographical boundaries; O5 Targets first another computer and the information within it; and, O6 Can result in cascading effects into the physical domains. While the DCO are almost the opposite: D1 No time for planning; D2 Can use both computers and physical means; D3 Defense measures need to be implemented immediately; and, D4 Infrastructure and data to protect are geographically linked.

Discussion

The question this paper tried to answer is whether Mission Command is appropriate for cyber space operations.

The answer must be a yes for Mission Command as a command philosophy and an "it depends" for Mission Command as a C2 Method.

Mission Command as a philosophy should permeate the entire organization as it creates independent individuals who can solve problems that arise quickly on their own. This creates a stronger and more flexible organization.

Mission Command as a method is related to control which support command and have dependencies on organizational structures, processes, technology, etc. The relevance of Mission Command to cyberspace operations as a method can be considered from several directions. First, it is a sensible response to a complex environment. Complexity theory suggests that the most effective way of solving dynamic and interrelated problems is by decentralized decision-making and action close to the source of the complexity (Czerwinski, 1998). At the same time, C2 requires a certain amount of competency and training. There is no point in giving subordinates freedom of operation when they simply do not know what to do.

When we are exposed to OCO the commander on the spot must act quickly and appropriately; probably in a novel manner, but one in which supports his superiors' overall intent. That justifies Mission Command as a C2 method for DCO when we are exposed to cyberspace attacks. Mission Command with decentralized authority is necessary in order to create a resilient and self-healing system. But we can see that in decisions that have an impact on the entire organization, it is more appropriate to have centralized decisions when senior managers usually have both the mandate to make such decisions and a better overview of the entire situation. Alberts, et al, (2001), mentioned above as alternate Command arrangements[6] to employ according to the situation.

In the majority of OCO, centralized decisions are required since the person making the decisions must be able to assess immediate effects but also secondary effects and consequences in the longer term, including political consequences. Some type of OCO should be preapproved by the strategic level but executed by the operational level as suggested by Carvelli (2018). The fact that the cyber domain and the digital landscape can be completely changed by updating e.g. software and we do not want to warn the opponent that we are interested in influencing one-specific target indicates the need for centrally direct control of OCO. In addition, we can assume that the targets we really want to influence are the most protected. This means a great

[6] Command arrangements are used by Alberts, et al, (2001) do define who commands whom, who has priority etc.

need for intelligence and good preparation for being able to lead an OCO, which speaks for the need for central and direct control.

The method of choice should be based on who has the competence to command in the situation, the best situation awareness, who has the authority to act and the responsibility to command.

In order not to create confusion, we should have different names of Mission Command as a philosophy and Mission Command as a method. The name of the C2 philosophy can keep the name Mission Command while it might be appropriate to term the C2 method as Mission Control.

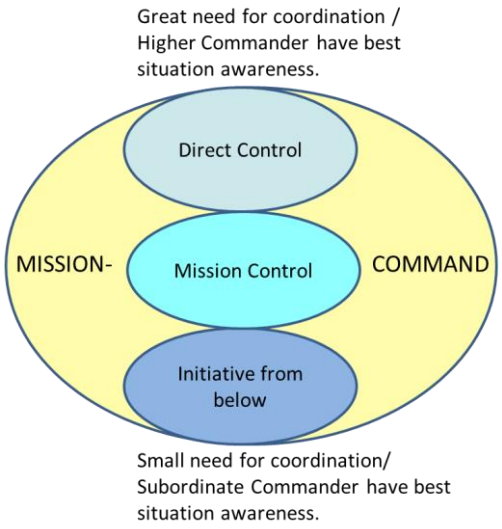

Figure 3 Mission Command and its three ways of control

Direct Control where higher commander provides tasks directly to the subordinates. Direct Control is used when there is a need for a high degree of coordination at time-critical operations. Direct Control means focusing on what is to be achieved in the short term and/or a limited part of the operational environment.

Mission Control where higher commander provides objectives for what the unit will achieve, but it is the subordinates who choose the means and methods to achieve the objectives. Mission Control is used when it is not required or possible with a high degree of coordination.

Initiative from below where higher commander's should support the initiative from subordinates and thereby achieve success. Initiatives from below are taken in situations where subordinate commanders have the best information about the situation or when the situation requires quick decisions. A precondition for initiatives from below is that higher commanders have communicated defined objectives and that there is mutual trust between command levels. During unexpected events, requiring initiatives from below, it is important that higher commanders support the initiative so that the entire organization can support it if necessary.

It is only through Mission Command as a philosophy that we can switch between Direct Control and Mission Control because an implemented such philosophy creates the prerequisites for both trust, intent, initiative and a common base. Subordinate commanders have to be trained for Mission Command methods to handle the switch between Direct Control and Mission Control since they must have the self-confidence to take their own initiatives, without detailed control

from higher echelon, when needed. To cope with initiatives from below, the entire organization must be trained in using that method.

The C2 method must be more flexible, the mission way of control should be complemented with a dynamic, and adaptive control policy for certain types of cyber actions. When choosing the C2 method it is important that the choice take into account both the SS need for action and the MS C2 needs. Some actions need a lot of coordination while others do not need it. Some immature organizations need more Control and guidance while mature and well-trained organizations need less Control. The C2-systems conditional view should consider all four conditions: competency, situational awareness, authority and responsibility before deciding C2 method.

Since the symptoms that we are exposed to a cyberattack usually are discovered locally, we can state that the cyber defense for DCO should be included in all units with a mandate for subordinate commanders to take their own initiatives and act quickly to minimize the consequences from the attack. On the other hand, we can also state that responsibility for commanding OCO should be higher echelons, as they are more able to understand the consequences of an offensive cyberattack and have better opportunities to coordinate extensive operations in time and space.

We suggest more research that examines the proposed Holistic Model of Dynamic Command and its suitability in different cases. We need more research to see if the model can be used for analysis of Command in other functions vital for public importance such as crises management, law enforcement, firefighting, emergency medicine, etc. We also suggest further research on how to decide who has the best situation awareness and who should thus be given a mandate to make decisions.

Another suggestion for further research is to test all views of representation that is built into the Holistic Model of Dynamic Command: conditional view, C2 functions view, system elements view and C2 products view. This could be done to design a C2 system for commanding different Mission Systems that are designed to meet the needs for actions that creates desired effects in the Situation System and thereby supports the transition from an unacceptable to an acceptable condition.

In this article, we have shown that Mission Command as a method of controlling CO is relevant under certain conditions depending on SS need for action and MS C2 needs. The article also shows that Mission Command as a philosophy is still viable for Commanding CO as long as we regard Command as a human activity. However, we need more research on what happens if we use AI for Command at different management levels, but that is a matter for future research.

References

Alberts, D., Gartska, J., Hayes, R. and Signori, D. (2001). *Understanding Information Age Warfare*. CCRP Publication Series, Library of Congress Cataloging-in-Publication Data, pp. 169 – 180.

Alberts, D. (2018a). *Multi-Domain Operations: What's New, What's Not, and the Implications for Command and Control.* Proceedings of 23th International Command and Control Research and Technology Symposium (ICCRTS), 6-9 nov, 2018. Pensacola, FL. USA.

Alberts, D. (2018b). *Cyberspace Operations: Is a Non-traditional C2 Approach Required?* Proceedings of 23th International Command and Control Research and Technology Symposium (ICCRTS), 6-9 nov, 2018. Pensacola, FL. USA.

Albright, D., Brannan, P. & Walrond, C. (2010). *Did Stuxnet Take out 1000 Centrifuges at the Natanz Enrichment Plant?* Institute for Science and International Security

Barius, P. (2012). *COPD och uppdragstaktik* [COPD and Mission Command]. Stockholm: Swedish Defence University.

Brehmer, B. (2005). *The Dynamic OODA Loop: Amalgamating Boyd´s OODA Loop and the Cybernetic Approach to Command and Control*. Proceedings of the 10th International Command and Control Research and Technology Symposium (ICCRTS).

Brehmer, B. (2006). *One Loop to Rule Them All*. Proceedings of the 11th International Command and Control Research and Technology Symposium (ICCRTS).

Brehmer, B. (2007). *Understanding the functions is the key to progress*. International C2 Journal, 1, pp. 211-232.

Broad, W.J. et.al. (2011). *Israeli Test on Worm Called Crusial in Iran Nuclear Delay*. The New York Times. January 15, 2011.

Carvelli, M.P. (2018). A Smarter Approach to Cyber Attack Authorities. Joint Force Quarterly (JFQ). 4th Quarter 2018, pp. 67 – 73.

Chen, T. and Abu-Nimeh, S. (2011). *Lessons from Stuxnet*. Computer, 44(4), pp. 91-93. Received from: http://openaccess.city.ac.uk/8203/

Czerwinski, T. (1998). *Coping with the Bounds. Speculations on Non-Linearity in Military Affairs*. Institute for National Strategy Studies, Washington DC, pp79-95.

Department of Defense. (2010). *Joint Terminology for Cyberspace Operations*. THE VICE CHAIRMAN OF THE JOINT CHIEFS OF STAFF. Washington.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors, 37, p.p. 32-64.

Finkel, M. (2011). *On Flexibility - Recovery from Technological and Doctrinal Surprise on the Battlefield*. Stanford University Press.

Flynn, M., & Schrankel, C. (2013). *Applying Mission Command through the Operations Process*. Military Review, March-April 2013.

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. Wired. Retrieved from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Granåsen, M., Barius, P., Hallberg, N., & Josefsson, A. (2018a). *Exploring Mission Command in a Concept for Future Command and Control - A Small State Perspective*. Proceedings of the 23rd International Command and Control Research & Technology Symposium (ICCRTS), 6-9 nov, 2018. Pensacola, FL. USA.

Hallberg, N., Granåsen, M. Josefsson, A., & Ekenstierna, C. (2018). *Framework for C2 development: Exploring design logic and systems engineering*. Proceedings of 23th

International Command and Control Research and Technology Symposium (ICCRTS), 6-9 nov, 2018. Pensacola, FL. USA.

Heerensdienstvorschrift 300/1 (1933). *Trüppenführung I. Teil*. pp. 10-11. Retrieved from Bundesarchiv-Militärarchiv, Freiburg.

Johansson, J.E., Carlerby, M. & Alberts, D. (2018). *A Suggestion for Endeavour Space Dimensions*. Proceedings of 23th International Command and Control Research and Technology Symposium (ICCRTS), 6-9 nov, 2018. Pensacola, FL. USA.

Joint Chiefs of Staff (USA). (2018). *Joint Publication 3-12. Cyberspace Operations.* Development, Concepts, and Doctrine Centre.

Knapp, E.D. & Langill, J. T. (2015) *Industrial Cyber Security History and Trends*. ScienceDirect. Retrieved from:https://www.sciencedirect.com/topics/computer-science/stuxnet/pd

Langner, R. (2011). *Stuxnet: Dissecting a Cyberwarfare Weapon*. IEEE Security and Privacy, May/June 2011, p. 49.

Lind, W. S. (1985). *Maneuver warfare handbook*. New York: Westview Press.

Macmillan Dictionary. https://www.macmillandictionary.com.

Marshall, S.L.A. (1947). *Men Against Fire: The Problem of Battle Command,* University of Oklahoma Press, 2000 first published 1947, p. 108.

Mattsson, Peter. (2003). *Upplysning, Romantik och Auftragstaktik*. pp. 55 In Cedergren, A & Mattsson, P.A (eds.). Uppdragstaktik – En ledningsfilosofi i förändring. Försvarshögskolan, Stockholm.

Nato Allied Joint Publication (2019). *ALLIED JOINT DOCTRINE FOR THE CONDUCT OF OPERATIONS (AJP-3).* Nato Standardization office, dated February 2019.

Norlander, A. (2011). *Cognitive Systems Modeling and Analysis of Command & Control Systems*. In Proceedings of the MODSIM World 2011 Conference and Expo. Virginia Beach, VA, USA. National Aeronautics and Space Administration. NASA/CP-2012-217326.

Norlander, A. (2019). *Strategies for Developing Agile Crisis Management Capabilities*. In proceedings of The 30th International Training and Education Conference. Stockholm, 2019.

Novet, J. (2017, August). *Shipping company Maersk says June cyberattack could cost it up to $300 million*. CNBC. Retrieved from: Page 71 https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattackcould-cost-300-million.html

O´Leary, M.M. (1999). *Auftragstaktik*. http://www.ducimus.com/Archive/auftrags-oleary.htm. 2002-11-03.

Perlroth, N. et.al. (2017). *Cyberattack Hits Ukraine Then Spreads Internationally*. The New York Times June 27, 2017.

Pigeau, R., & McCann, C. (2001). *What is a Military Commander?* pp. 394-413 in P. Essens, A. Vogelaar, E. Tanercan & D. Winslow (Eds.). *The Human in Command: Peace Support Operations.* Amsterdam: Mets & Schilt.

Pigeau, R. & McCann, C. (2002). *Re-conceptualizing Command and Control*. Canadian Military Journal, Volume 3, Number 1, spring 2002, pages 53-64

Pogoson, A. I. (2018). *Issues, Trends and Challenges in an Emerging Global Power Structure.* Canadian Social Science, 14(2), 5-15.

Raitasalo, J. (2019). *America's Constant State of Hybrid War*. The National Interest. National Interest.Org.

Rosenbaum, R. (2012). *Richard Clarke on Who Was Behind the Stuxnet Attack*. Smithsonian Magazine. Received from: https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/

Silgado, D.M. (2018). *Cyber-attacks: a digital threat reality affecting the maritime industry*. World Maritime University. World Maritime University Dissertations. 11-4-2018.

Singer, P.W. and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press Inc. New York, United States.

Storr, J. (2003). A Command Philosophy for the Information Age: The Continuing Relevance of Mission Command. Defence Studies, Vol.3, No.3, pp. 119-129.

Teske, K, Miller, M. Guerin, P. and Lauver, J. (2018). *Decoupling Command from Control - Making the term C2 Stronger.* Proceedings of 23th International Command and Control Research and Technology Symposium (ICCRTS), 6-9 nov, 2018. Pensacola, FL. USA.

US Army. (2012). *Mission Command - Army Doctrine Reference Publication No. 6-0* (ADRP 6-0). Headquarters, Department of the army, Washington, DC, 17 May 2012.

US Army. (2017). *Army Doctrine Publication No. 3-0 Operations* (ADP-3-0). Headquarters, Department of the army, Washington, DC, 6 October 2017

Ernst van den Bergh (1906), *Die seelischen Werte im Frieden und im Kriege* (Ethical values in peace and war), a study in Militär-Wochenblatt 91 (Military weekly) (91, 1906), Beiheft 6 (insert 6), 233, as quoted in Leistenschneider, 95.

Weiner, N. (1961). *Cybernetics or control and communication in the animal and the machine.*, The M.I.T. Press. Cambridge, Massachusetts

Widder, W. (2002). *Auftragstaktik and Innere Führung: Trademarks of German Leadership*. Military Review, 82(5):3-9.

Williams, P. et.al. (2016). *Cyberspace: Melevolent actors, criminal opportunities, and strategic competition*. Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College.

Wirtz, J.J. (2017). *Life in the "Gray Zone": observations for contemporary strategists*. Defense & Security Analysis, 33(2), 106-114.