Article received in May 2016 and accepted for publication in May 2016

CONSIDERATIONS ON COMMAND AND CONTROL

CONSIDERAÇÕES SOBRE COMANDO E CONTROLO

Rodrigo Damasceno Sales
Major
Master's Degree in Military Science
Instituto Meira Mattos
Escola de Comando e Estado-Maior do Exército
Rio de Janeiro, Brasil
rdsales@gmail.com

Luiz Rogério Franco Goldoni
Teacher and Researcher
PhD in Political Science
Instituto Meira Mattos
Escola de Comando e Estado-Maior do Exército
Rio de Janeiro, Brasil
luizrfgoldoni@gmail.com

Abstract

The advancements in Command and Control systems (C2) have influenced the 'face of battle' since times immemorial. The concepts known as 'Network Centric Warfare' and 'Cyberwarfare' feature new weapons, actors and forms of combat, posing new challenges to a State's defence systems. The present research paper shows, by means of a literature survey, the different C2 definitions and concepts, in an analysis of its importance and historical evolution. Finally, we will examine Network Centric Warfare, Cyberwarfare and their implications.

Keywords: Command and Control; War; Network Centric Warfare.

Como citar este artigo: Sales, R., Goldoni, L., 2016. Considerations on Command and Control. *Revista de Ciências Militares*, maio de 2016 IV (1), pp. 303-326.
Disponível em: http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes.

Resumo

Evoluções em sistemas de Comando e Controle (C2) impactam desde primórdios a "face da batalha". A chamada "Guerra Centrada em Redes" e a "Guerra Cibernética" apresentam novas armas, atores e formas de combate, impondo desafios inéditos aos sistemas de defesa das nações. O estudo em tela, mediante pesquisa bibliográfica, apresenta diferentes definições e conceitos de C2 e analisa sua importância e evolução ao longo da história. Ao final, investiga-se a Guerra Centrada em Redes, a Guerra Cibernética e suas consequências.

Palavras-chave: *Comando e Controle; Guerra Centrada em Redes; Guerra Cibernética.*

Introduction

'Ciberwarfare' (Cyber W) is a reality today, as demonstrated, for instance, by the events that paralysed operations in a uranium-enrichment plant in Iran. On the other hand, 'Network Centric Warfare' (NCW) is an important evolution in the field of Command and control (C2), which has been increasingly migrating its systems to computerised systems, rendering them vulnerable to the actions of 'hackers'. The present work aims to analyse, by means of a literature survey, the concept of Command and Control and the challenges it poses. First, we will present definitions and concepts on C2; next, we will examine the development of Command and Control in warfare. Finally, we will analyse how advances in C2, NCW and Cyber W influence national defence and warfare.

1. Initial Definitions

In order to understand the meaning of the term 'command and control', we must consider the individual definitions of 'command' and of 'control', which depend both on the operational level being examined and on who is using them. This section will begin by presenting the 'official' definitions adopted by the Defence institutions of Brazil, Portugal and the United States of America (USA). Next, an analysis will be made of the academic perceptions on the term. The numerous definitions that will be presented were deemed necessary because the expression is constantly evolving, and its specific characteristics depend on the technological level of those who use it[1].

According to the doctrine of the Ministry of Defence (MD) (BRASIL, 2014b, p. 15), Command and Control (C2) can be defined as a science and an art[2] that deals with the operation of a chain of command. This conception includes three basic components:

[1] For example, a C2 system in the US Army has, in principle, unrivalled characteristics when compared with those of other countries.

[2] Fonseca (2002, p. 10) states that science is 'knowledge produced by logical reasoning combined with practical experimentation. It is characterised by a set of models of observation, identification, description, experimental research and theoretical explanation of phenomena. Art can be associated with personal attributes, and is linked to individual talent.

1) legally vested authority supported by an organisation, from which the decisions that represent the exercise of command, and into which the information[3] required for the exercise of control flows;
2) a decision-making process system that allows the issuance of orders and enables the flow of information, supporting the mechanisms that guarantee full compliance with orders;
3) a structure that includes the personnel, equipment, doctrine and technology needed for the monitoring of operations by a superior vested with authority.

The terms 'command' and 'control' are intrinsically linked and are often used together; however, they are not synonymous. 'Command' consists of: authority, decision making and leadership; it resides in the figure of the commander; and, as it is based on personal characteristics, exists in each person to a varying degree, and is therefore considered an art (PORTUGAL, 2014, p. 7). 'Control' is considered more of a science than an art, in so far as it depends on objectivity, data, events, and methods of analysis, therefore providing support to the art of command (PORTUGAL, 2012). Thus, the main task of a military commander is to implement C2 on his troops, by employing the art and science of war.

In the opinion of the Brazilian MD, the goal of the 'command' activity is to establish hierarchical relationships that must be maintained at all stages of a military campaign. In turn, 'control' aims to 'establish the procedures enforced by Operational Command to control the actions of subordinate forces, providing the flow of information needed to monitor operations' (BRASIL, 2011a, p. 123).

For the Brazilian Army (BA), the objective of 'command' is decision making and that of 'control' is effectiveness of command or mission accomplishment (BRASIL, 2015, p. 2-1). Meanwhile, the Portuguese Army defines 'control' as the regulation of forces and combat functions to fulfil a task assigned by a commander, thereby enabling decision-making and planning adjustments (PORTUGAL, 2014, p. 7).

In 1997, in its systematic analysis of the term 'C2', the *Manual do Exército Brasileiro C-11-1 - Emprego das Comunicações* [Brazilian Army Manual C-11-1 - Use of Communications] mentioned the new computerised scenario and the new requirements it entailed, like the use of sophisticated computer networks to speed up the flow of information during combat, streamlining the decision-making process. The document also states that 'the system will be more or less effective depending on the effectiveness of the communications and computing capabilities' (BRASIL, 1997, p. 3-1).

A previous version of the manual of operations of the BA, C100-5 (BRASIL, 1997a), described C2 as an operating system, and its function was described as follows:

> *The system allows commanders of all ranks to visualise the battlefield, assess the situation and conduct the military actions necessary to win. It also enables*

[3] The term 'information', as used in this paper, is related to data and, by analogy, the term information flow refers to the flow of messages, or flow of data.

> *the exercise of command by linking communications between command posts and between commanders and their general staffs when the former are away from their command post. Communication is the key element in the exercise of command and control in combat (BRASIL, 1997a, p. 2-13).*

The BA later defined C2 as a combination of human and material resources, allied to certain procedures, intended for command, control and communication with friendly forces, as well as for obtaining information (BRASIL, 2003, p. C-13). Eight years later, the doctrine of the MD further developed the concept by emphasizing that C2 'comprises the provisions regarding control of operations, command hierarchy, and instructions related to communications' (BRASIL, 2011a, p. 54/208).

In 2015, the Brazilian Army adopted for the first time a pure Command and Control manual by distinguishing the term 'C2' from the previous manuals of operations and communications. It presented the following definition:

> *Command and control consists of the exercise of authority and direction by a commander over assigned forces in the accomplishment of a mission. It enables coordination between the issuance of orders and directives and the gathering of information on the progress of a given situation, and of the actions taken (BRASIL, 2015, p. 1-2).*

When one considers these definitions, which are in fact rather similar, it is clear that they initially focus on the figure of the Commander, who requires a vast communications system to develop military operations. The term 'C2' was altered in 2015 to reflect a greater focus on the flow of information required by Commanders to guide their decisions. Thus, an efficient system should be deployed to process the data fed into command.

According to the provisions of the MD, C2 requires peculiar characteristics such as interoperability, reliability and flexibility (BRASIL, 2014b). Its basic principles are unity of command, delegation of authority, simplicity, and security.

Thus, in the field of national defence, in particular for the BA, C2 is the key element in the use of Land Forces in military operations, as they require complex means of coordination to achieve success. Support to communications, which are the physical base of the system, directly influences the efficiency of a military organization's C2. In practice, the two definitions of C2 appear to be closely related, as in fact they are, the only differences between them being the agency that employs them and the time in which they were proposed.

In turn, the *Doctrinal Publication of the U.S. Marine Corps - MCDP 6* (USA, 1996), defines C2 as the means by which a commander recognizes what needs to be done and sees to it that appropriate and corresponding actions are taken. Thus, the exercise of C2 is essentially an attribution of a commander, and the C2 system is responsible for giving meaning and harmony to all other combat functions. This approach reveals a third defining quality of C2, as the term, previously described by Brazil and by Portugal as a science and an art, is now defined by the US as a means.

Another definition of C2 is the one described in the *Field Manual FM 1-02, Operational Terms and Graphics* (USA, 2004) of the US Army. This document describes C2 as the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission, which is done by means of a C2 system. This definition clearly focuses on 'exercise' as the term's fourth characteristic, evidencing the different interpretations of Brazil, USA and Portugal.

In 2009, the *Dictionary of Military and Associated Terms of the US Department of Defence* (USA, 2009) described C2 as the exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of a mission. The American doctrine states that C2 functions consist of anarrangement of personnel, equipment, communications, facilities, and procedures employed by a commander to plan, direct, and coordinate and control forces and operations in the accomplishment of the mission.

In the academic sphere, the origin of the term 'C2' was linked to the emergence of modern warfare techniques, which 'forced armies to develop elaborate C2 and communications systems to orchestrate the various arms on a complex battlefield' (HOUSE, 1984). In a workshop presented at the University of Campinas[4], the term C2 was described as follows:

> *Command is the expression of authority exercised by a superior officer over his subordinates to achieve a given objective. Control is the term used to describe the structures and processes that allow orders to be transmitted and understood, also enabling risk management. That is, C2 are interconnected concepts, vital for the conduct of military activities*[5].

Another definition, this one by Sproles (2001), states that a C2 system consists of personnel, information and support. Afonso and da Silva (2013, p. 11) also explain its usefulness:

> *[...] actions that are commanded and controlled in an integrated manner, relying on C2 techniques, allow one to achieve situational awareness in a rapid and accurate manner, allowing those in command positions to employ the means available in a more rational and objective manner, undoubtedly leading to a more rapid and accurate response to any challenges that may arise.*

In the presence of so many concepts, it is noteworthy that at their 'core' they are intrinsically linked to the decision-making process, be it a typically military process or otherwise, ranging from complex security activities at high government levels to activities related to the management of military personnel, and even simple tasks such as those of a leader in a business meeting by video-conference. The definitions presented so far reveal that the terms 'command' and 'control' are interconnected. The first term focuses on decision and the second aims to lend effectiveness to the first.

---

[4] We could not identify the lecturer who prepared/presented the lecture '*Princípios Básicos de Operações Militares*' [Basic Principles of Military Operations], which we cite in this paper.

[5] Retrieved from: <http://www.students.ic.unicamp.br/~ra092208/downloads/workshop.pdf>. Accessed 17 November 2015.

When the concepts described are analysed from a military perspective, they imply the presence of a superior, a chain of command, a doctrine defining the rules of interaction, and the flow of information across that chain of command. Thus, the term C2 has become synonymous with these premises (ALBERTS, 2009).

Alberts and Hayes (2006)list seven functions involved in the exercise of C2:

1) establishing intent;
2) determining roles, responsibilities and relationships;
3) establishing rules and constraints;
4) monitoring the situation and progress;
5) motivation and trust;
6) training; and
7) provisioning (Logistics).

Thus, command sets the conditions under which C2 will operate. For the sake of simplicity, command should determine the C2 processes while control assesses whether the current and/or planned efforts are consistent with the objectives. If adjustments are required, the function of control is ensuring that those adjustments are made within the guidelines established by command. The essence of control is to keep the values of the specific elements of the operational environment within the bounds established by command, primarily in the form of intent (ALBERTS, HAYES, 2006, p. 59).

Alberts and Hayes (2006) created a table describing the conceptual C^2 model shown below:

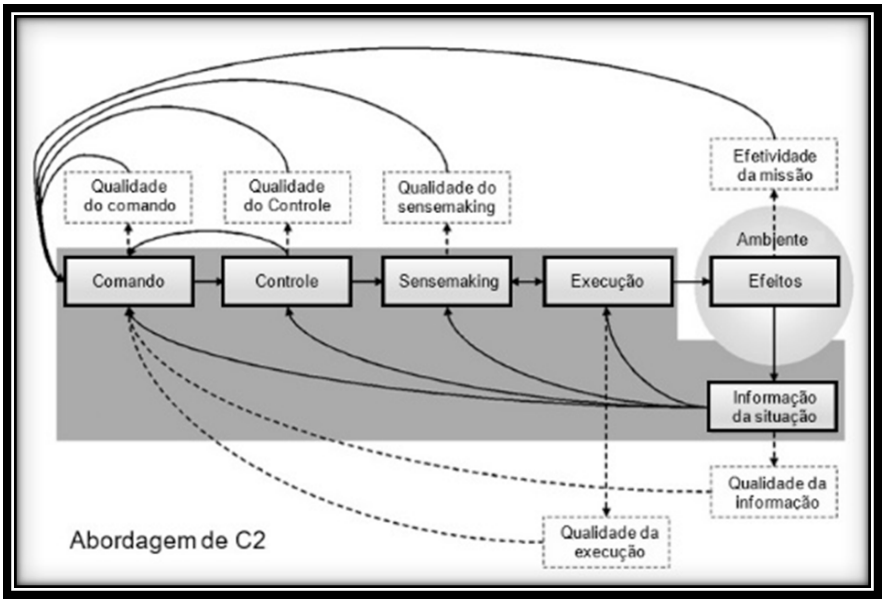

Figure 1- C2 Approach

Source: ALBERTS; HAYES, 2006, p. 53

Lawson (cited in (ORR, 1983)) describes the C2 process in the figure below, representing a loop of actions carried out by a commander and the influences received:

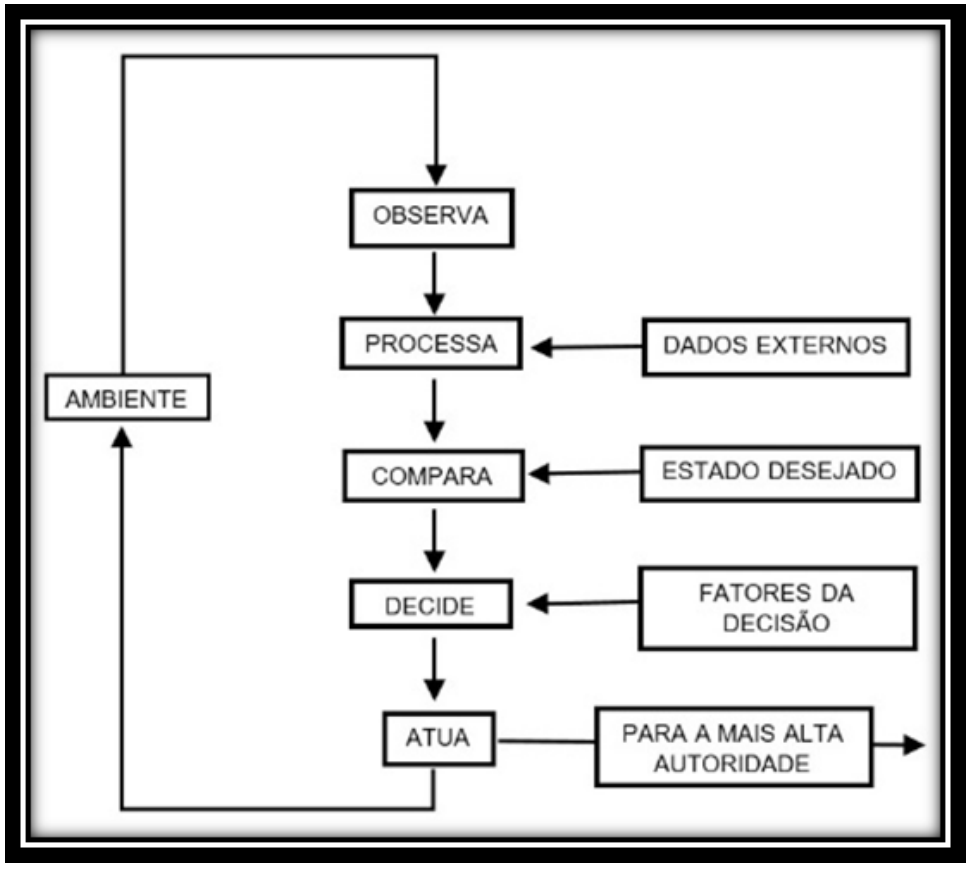

Figure 2- Conceptual C2 model, according to Lawson

Source: Lawson cited in ORR, 1983, p. 33.

The continuous decision-making process is known in the military as Boyd loop or OODA[6] (Observation-Orientation-Decision-Action)[7] and is equivalent to the PDCA (Plan-Do-Check-Act) cycle that originated in the business community (BRASIL, 2011b, p. 64). This loop is used to obtain advantages in combat, in the sense of acquiring vital information before the opponent, which favours the maintenance of combat initiatives. The Boyd loop was created with the purpose of focusing the understanding of how C2 activities are developed (BRASIL, 2014b, p. 21).

[6] The OODA Loop was developed by Colonel John Boyd after analysing the success of the F-86 US fighter aircraft compared to the Soviet MIG-15. Although the MIG was better at climbing and manoeuvring, the American aircraft won more battles because, according to Boyd, the pilots had a higher field of vision. This gave the pilots a competitive edge because it allowed them to assess the situation better and more rapidly than the opponent.

[7] The C2 doctrine of the BA refers to the OODA loop as C2 Loop (BRASIL, 2015, p. 1-2).

Figure 3- Boyd Loop - OODA

Source: BOYD, 1987.

The table below shows the evolution of the BOYD loop, demonstrating the impact of the technological modernisation of C2 capabilities:

Table 1 - Evolution of the OODA Loop

	1780's	**1850's**	**1940's**	**1990's**	**2000's**
Note	Telescope	Telegraph	Radio, radar	Sensors	Whole networks
Orientation	Weeks	Days	Hours	Minutes	Continuous
Decision	Months	Weeks	Days	Hours	Immediate
Action	1 Season	1 Month	1 Week	1 Day	1 Hour or less

Source: Cruz, 2006 cited in Leske, 2013, p. 58.

According the Boyd Loop (1987), in combat, where C2 activity is evident, it is essential to have a faster decision cycle than the opponent, so that the time lag gives rise to opportunities and so any advantages can be exploited effectively (FORD, 2010). Thus, the evolution of the loop shows that speed in the execution of orders and a C2 characterised by fluidity are determining factors for success.

Acting first against the opponent creates advantages that are continuously and successively incremented every time the decision-making loop is completed. This also damages the C2 capability of the adversary, and sooner or later will inevitably result in the complete collapse of their ability to conduct actions.

It should also be noted that C2 is ruled by guiding principles, from planning to implementation. Some of these principles, provided for in the Brazilian doctrine (BRASIL, 2014b, p. 17-18/44), are the following:

- **security** - *consists of denying or hindering unauthorized access to information which belongs to friendly forces, restricting the opponent's freedom of action to attack sensitive points of the C2 system;*
- **flexibility** - *it should be possibly to rapidly reconfigure the C2 system in order to respond to an imminent change of environment. The Flexibility Principle can be achieved with an intelligent system design and by using fixed, mobile and transportable facilities;*
- **reliability** - *a C2 system will be trustworthy if it has the ability to survive and maintain effectiveness when exposed to destabilizing events caused by the operational environment, by internal damage, or by acts of God;*
- **continuity** - *C2 systems must operate continuously. This principle directly influences the allocation of resources - human and material - at all levels. For a C2 system to meet the continuity principle, the planning stage should always consider the redundancy of resources and links;*
- **speed** - *C2 systems must bring speed to the decision-making process;*
- **integration** - *a C2 system of a certain level is not isolated; it is part of the system of the level above it and encompasses the systems of the subordinate levels; it must also have the ability to share information with peer forces.*

These different conceptual aspects of C2 reveal that Man is the key element in the operation of each of the systems introduced by the above definitions. The decision-maker, the central figure that is the raison d'être for C2, must have the expertise required for the function. Otherwise, the data presented by the system will do no good. The operators of equipment that make up the physical structure of the system must also have proper training (YARMIE, 2003) to keep the flow of information active.

2. History of Command and Control

Once the conceptual basis of the theme has been established, we may now take a further step in understanding C2 by researching its origins and how it was employed. Although the term and its definitions did not yet exist, C2 dates back to ancient history, when warlords used conventional signs or had systems of messengers at their disposal to exercise command over their troops, receive orders and inform their superiors on how the fighting was progressing.

A symbolic action was immortalized by the Greek soldier Pheidippides in 490 BC, during the war between Greece and Persian, who ran a distance of over 40km on foot from Marathon to Athens, Greece, to deliver the message of the Greek victory. Thus, C2 is indelibly inscribed on the origin of a classic athletics trial, the Marathon, which traditionally marks the end of the Olympic Games.

Many of the great military leaders in history such as Napoleon, Alexander the Great, Genghis Kahn, Moltke, the Duke of Caxias, Eisenhower, Churchill and Hitler realized that, in order to succeed in their endeavours, they would have to improve their control over their troops, developing unique enhancements to the C2 systems of their respective times (SCHERMERHORN, 2006, p. 8-22; DORATIOTO, 2002; BOSE, 2006; WEATHERFORD, 2010; ALBERTS, 2009; HUGHES, 1993).

In 336 BC, Alexander the Great, also known as Alexander III of Macedon, was crowned king of the ancient Greek kingdom of Macedon. Alexander spent most of his years in power carrying out a series of military campaigns across Asia and north-east Africa. He created one of the greatest empires of the ancient world, stretching from Greece to Egypt and north-west India. In the words of Bose (2006, p. 87):

> *Much of the military success of the Macedonians was due to efficient communication during battle, allowing the information to arrive accurately and on time to the combatants. 'Each element of his battalions had the task of achieving a certain predetermined purpose and communicated through a combination of conventional signs and messengers'.*

According to Weatherford (2010), circa 1200, History's greatest conqueror, Genghis Kahn, devised a system of communications composed of couriers and horseback messengers to streamline his information system and allow greater efficiency in the employment of C2 on his troops. In 25 years, Kahn subjugated more lands and people than the Romans did in 400 years, and, at his peak, he led an empire of about 19 million contiguous km^2, an area almost the size of the African continent (WEATHERFORD, 2010).

A consistent development of C2 emerged in the sixteenth century with the use of a personal advisor by Gustavus Adolphus, which was continued in the nineteenth century with Napoleon use of a General Staff- although his egocentric personality weakened the system of command by subjecting it to the authority of a single person (VAN CREVELD, 1985, p. 63-65). In fact, the modern C2 design begins with Jomini, who considers that a General Staff and a system to control and direct the operations of war (current C2 system) are 'essential

conditions [that] concur in making a perfect army' (JOMINI, 2007, p. 32). Since then, C2 has been considered a key component in the development of battles.

In the American Civil War (1861-1865), the use of the telegraph, invented in 1843 by Samuel Morse, was implemented as the primary means of communication at great distances, facilitating the flow of information, as the railway crossing the country facilitated military logistics and C2 activities such as messenger traffic.

In Brazil, between 1864 and 1870, during the War of the Triple Alliance, the Duke of Caxias, Luis Alves de Lima e Silva, also concerned himself with the use of C2, as he saw in it a way to tilt the balance of war to the Brazilian side:

> *The use of observation balloons and telegraph facilities implemented by Caxias not only made communications faster, they also enabled the advance of the troops into enemy territory and the conquest of the most important obstacle to the advance of the allies in Solano Lopez's homeland: the Fortress of Humaitá (CORREIA, 2014).*

In the Franco-Prussian War (1870), Moltke (who felt great affinity with the classic strategy doctrines of Clausewitz and Jomini) used the railways and the telegraph to perform manoeuvres of a magnitude the likes of which had never been seen before by engaging the enemy's front line and reserves simultaneously (MAGNOLI, 2006, p. 314-315). His concern for communicating via telegraph with his troops, who were projected at long distances by the railway, is proof of the importance the Prussian General placed on C2, which he believed would influence the new dimensions of manoeuvre. Moltke's legacy to military history consisted of his doctrine and of the lesson that ongoing communications between commanders and commanded are greatly relevant to combat and are indispensable to effectively conduct and control actions, so that the desired end state, the primary objective of the operation, can be achieved with due success (HUGHES, 1993).

In World War I (1914-1918), C2 was implemented by linking the theatres of operations through telegraph lines, by using railways as traffic lines, and by a new medium of communications: the telephone, invented by Graham Bell and patented in 1876. The transmission of messages via telephone increased the speed of information and C2 efficiency.

The importance of C2 is evidenced by several events of World War II (1939-1945). In the beginning of the war, the Axis troops quickly dominated nearly all of Europe, even advancing into Africa and Russia. The Nazi-fascist forces managed to extend their domain to thousands of kilometres and were able to reap the rewards of applying a destructive and innovative war tactic known as ***blietzkrieg***. With regard to the issue of C2, it should be noted that the Germans used a robust communications system to coordinate and control troops projected at great distances, mainly by using the radio, invented by Guglielmo Marconi and patented in 1896. The Axis countries also used the telephone and the telegraph, as in the previous war; however, the great German innovation was the integration in the fighting of an important protection mechanism for its C2 system: the Enigma machine. This equipment added

encryption to transmitted messages, rendering their content indecipherable should they be captured by the enemy. This afforded them a crucial strategic advantage for many years into the war, as the C2 structure was preserved by maintaining confidentiality in information and operations (HODGES, 2014).

To allow the use of allied troops in areas dominated by the axis in Europe, Asia and Africa, it was also necessary to implement a large-scale C2 system. The system allowed the control of troops by relying on technological support mainly from the USA and England.

To tip the war in their favour, the allies faced the considerable challenge of dismantling the C2 of Hitler's troops and denying the surprise factor to the German attacks. To that end, Churchill ordered the development of a technology that could break the encryption of the Enigma machine, which occurred in 1943, with an invention by Alan Mathison Turing. The equipment, which is considered the genesis of computer science, was known as the Bombe machine and allowed the allies to decrypt the enemy messages, revealing their intentions hours in advance.

Turing's discovery helped England prepare against several Nazi attacks, and it is speculated that the invention shortened the war in over two years, saving thousands of lives. Winston Churchill, then Prime Minister of England, went on to say that Turing had made the greatest contribution to the Alliance's victory against Germany (CARRERA, 2015).

In recognition for his achievements, Turing was later acclaimed as the father of computing. This striking episode demonstrates the relevance of C2. As we could see, it is clear that technological developments have contributed to increase the number of troops employed in the battles, and also modified the theatre of operations, which had once been relatively small, but now had been increased to a level never seen before, acquiring a global dimension. It should be noted that, although the use of radio in WWII solved the mobility problems encountered in WWI, where communications were established by telegraph, the exercise of C2 for expeditionary troops did not become easier (SMITH, 2010, p. 41).

The year of 1962, during the Cold War, was marked by the episode of the Cuban missile crisis, which involved the main world powers, the USA and the Soviet Union. The crisis highlighted numerous C2 problems that could trigger a nuclear disaster of major proportions. According to Pearson (2000, p. 51), the event boosted the creation of a more comprehensive C2 system, at the request of US President J. F. Kennedy. Therefore, in 1979, the World Wide Military Command and Control was created in the US, becoming a crucial element in US national security (USA, 1979), combining sensors, computers, command posts and communication networks of different AF in a single system, improving the situational awareness of American leaders.

When considering modern conflicts, it is clear that C2 is still under development and that its importance is gradually on the rise due to the characteristics of new forms of combat. In the Gulf War (1991), one of the main objectives of the US offensive was to 'suppress Iraqi command and control' by means of an air campaign that would set the stage for the ground attack (USA, 2010, p. 28, tradução e grifo nossos).

Ten years later, the US deployed operation Enduring Freedom during the events that followed the September 11 attacks. In the early attacks on the Taliban in Afghanistan, the North Americans focused their attention on dismantling the C2 of the opponent by using air strikes, as they had done in the Gulf. The technological advancements enhanced the agility of the post-September 11 operations. While in 1991 the information processing time entailed in an interval of three days between the identification and bombing of a target, in the second Gulf War (2003), only 45 minutes passed from the moment the information was received of Saddam Hussein's meeting with military commanders and the time the satellite-referenced location was bombed (BOOT, 2003, p. 52).

Much of the success of Operation Neptune Spear, which carried out the deadly attack on Bin Laden, can be attributed to the use of a global C2 system (SCHLOSSER, 2015). The most advanced means of communication were used, such as Digital Globe and Geo Eye satellites to monitor the area of operations and feed the C2 systems; images taken by cameras installed in the helmets of the soldiers were sent to the Pentagon and to the aircraft on site (LELE, 2011, p. 129-130). These innovations brought further integration to combatant forces and further enhanced the situational awareness provided by C2 systems, which began operating within increasingly dense and complex networks. This new way of operating in battle was defined as Network Centric Warfare (NCW)8, which we shall discuss later.

The events of the Gulf and of Afghanistan revealed the importance of suppressing the enemy's C2 in the early stages of the conflict in order to facilitate the advance of the troops. It is noteworthy that the USA's objective in launching an attack on the Iraqi C2 system was to dismantle the forces in that country, thus neutralising their ability to conduct military operations:

> *The conquest of major cities was not conducted in the conventional way, in which the infantry engages in house-to-house fighting. Instead, intelligence,* ***command and control warfare****, information warfare and joint infantry-tank operations were carried out, avoiding as much as possible the disembarkation of Marines (PORTUGAL, 2008, p. 29, grifo do autor).*

This is an aspect of the evolution in warfare, which ceased to be conducted like the battle of Aachen (World War II), where an entire city was destroyed to allow the passage of troops. Today, dismantling an enemy C2 is the step before the ground offensive with kinetic means, in what is known as Command and Control Warfare. One of the goals of this type of warfare is to increase military efficiency in order to minimize casualties in combat.

The evolution of C2 contributed to change the way of operating in armed conflicts and transformed the forms of manoeuvre and employment of combat forces. Force integration became more effective due to the combination of the various communication networks, sensors and assets. This development may be related to the intent of minimising the number of casualties, especially among allied forces and civilians.

[8] According to Luddy (2005, p. 3), NCW: 'Represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner'.

3. Commandand Control Today

The twenty-first century brought with it new challenges; today's military missions are different from those of the past. They became more complex and dynamic, requiring collective capabilities and joint efforts by many organizations in order to succeed (ALBERTS, HAYES, 2006).

Due to the new perceptions on the evolution of C2, which influence the quality and efficiency of different systems, since 2006, a North Atlantic Treaty Organization (NATO) research group has attempted to define a conceptual C2 model that provides agility in the processing of information to deliver quality, timely results. According to these researchers, in order to obtain a quality C2 system, its functions must be well developed. C2 is meaningless without a mission or a purpose (CORDEIRO, 2014). In addition to an objective, it is also important to specify the risks that are acceptable for the achievement of the mission. Conducting infeasible missions is a failure in command. Therefore, a commander must define the desired end state in clear terms. The research group also stated that a quality C2 requires monitoring the situation at all times, so that any changes can be acknowledged and adapted to. All those involved must also interact with readiness, so that they may contribute individually to the final result.

The new C2 definitions imposed by the environment in the twenty-first century require specific training and education in order to better prepare the human resources involved. It should also be noted that C2 systems involve hardware and software technology, which is generally expensive and needs consistent financial support for development and sustainability.

In addition to the main concerns with the structure of the C2 system in warfighting, its importance is also reflected in the influence of the media. The 1991 Gulf War was the first time an armed conflict was broadcast live on television. The television coverage brought excitement to spectators, who could follow the war in real-time. The transmission of the war live on CNN, which employed previously developed C2 assets such as satellite, was so important and innovative the company was forever engraved in the history of world journalism[9].

Mention must be made of the impact of public opinion, which has become one of the Centres of Gravity that must be conquered whenever components of the Land Force are used, as communication with the national and global societies determines the dominant narrative (BRASIL, 2014a, p. 2-6). CNN viewers were exposed to the station's influence and its journalistic perspective[10]. In that conflict, great care was taken both to minimise and to show the allied casualties in combat in order to secure public support. This issue is a crucial point for C2 in warfighting, as it can potentially minimize casualties.

---

[9] Retrieved from: <http://www.fca.pucminas.br/omundo/interesses-e-fatos-por-tras-da-cobertura-da-guerra-do-golfo/>. Accessed: 21 February 2016.

[10] It should be noted that the media-public opinion relationship is not new to the 'morale' of a population, to support for the cause and, consequently, for the 'good progress' of the war. The film *The King's Speech* (2010) shows the importance of radio during World War II. Perhaps the most prized and famous photo that influenced public opinion in the Vietnam War is that of Kim Phuc, the little Vietnamese girl running naked after a napalm attack in 1972.

The exercise of command and control is increasingly difficult due to the complexity and the peculiarities of the combat environment, which has migrated to urban areas. It requires more planning and a detailed examination of the use of means, as well as continuous improvement and adaptation (YOUNG, 2011). Indiscriminate bombings and civilian casualties are not well accepted by public opinion and by the international community, and can thus harm military action. Although this paper does not intend to analyse issues related to the doctrine of war, a superficial approach to this knowledge was deemed necessary, as C2 is intrinsically linked to the art of command.

Nowadays, the C2 development has reached a high level of complexity, with the use of high-tech equipment, such as those in the military C2 apparatus used by the Americans in Afghanistan and in other target countries of its war on terror policy. On these occasions, most American tactical actions are developed in a relatively decentralized manner, often performed by small patrols of soldiers, which shows an evolution in the way of fighting.

In the history of war, troops have been employed in a decentralised manner; however, there have always been mechanisms to guarantee C2 for combat fractions, albeit in rudimentary form. It can be said that technological modernisation of C2 structures potentiated the decision-making process in a proficient and reliable manner, to the lowest levels of command. This allowed greater freedom of action, job flexibility, and effectiveness in the development of operations and compliance with mandated tasks (DEMPSEY, 2011). The success in several actions by small forces of the US Army in Afghanistan, in a decentralized manner, in caves and over extremely rough terrain, resulted from the effective C2 checked at all levels (Bahmanyar, 2004; Raugh, 2011) . Thus, neglecting the preparation of the troops for the use of a C2 system, which aims to act on operational environments characterized by dynamism of actions, complexity and decentralization of execution of the tasks will probably result in failure.

C2 must adapt as needed, in accordance with the characteristic principle of flexibility. In the Brazilian Army, C2 is used to maintain the land forces in operations, both administratively and operationally. In military operations, the Tactical Communications System (SISTAC) is activated to allow C2 under any circumstances. The MINUSTAH military operations, Guarantee of Law and Order Operations (GLO) and interagency operations are good examples of this.

The BA considers and binds C2 to the six existing combat functions: C2, Movement and Manoeuvre, Intelligence, Fires, Protection and Logistics (BRASIL, 2015). As in Brazil, the *US Army FM 3-0 - Operations Field Manual* (USA, 2008) ranks C2 as one of six combat functions. It defines C2 as the systems and related tasks that support commanders in the exercise of their authority and direction. It is through this function that commanders integrate all other functions for the achievement of the missions, whatever their nature.

The US Army recently redesigned its operational procedures with the aim of developing, training and instructing its members in the best possible way, so that they could better respond to the increasing current challenges, which are characterised by fighting in urban environments. In this context, the exercise of C2 is currently considered a key factor for the performance of any task.

The structure that allows the development of C2 systems, entitled physical base, comprises both equipment and facilities. This conglomerate was entitled Command and Control Centre (CC2) and is the embodiment of the concepts described. These centres are characterised by the presence of advanced technology and the use of communications and computing, and are immersed in a highly complex technical environment.

The NATO[11] concepts specify that a CC2 should enable integration based on the C4ISR concept (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). It is vital that the different combat functions can be integrated with a real-time flow of information, and are able to provide a broad situational awareness of the area of action to the command of the operation.

The C2 process is very similar in military and non-military corporations, as well as in other types of companies. In those organizations, the CC2 are the basis of the communications system, and are in fact the concentrators of the information that is made available to the heads and directors. In general, current C2 systems include voice communication, real-time monitoring of imagery of areas of interest through a system of cameras or satellites and geopositioning, among other tools designed to increase quality in decision-making by reducing the time elapsed between the initial awareness of the facts and the response.

Other organizations that use C2 systems are related to residential security services, vehicle monitoring GPS systems, groups linked to logistics, among other activities, including government entities such as the Brazilian Institute of the Environment and Renewable Natural Resources (IBAMA). This body contributes by combating deforestation, monitoring forest areas through a C2 system designed for that purpose, as described in the excerpt below:

> *Brazil's efforts to improve the process of enforcement of laws and the* ***monitoring*** *of forest areas prevented the deforestation of approximately 59,500 km2 of Amazon forest between 2007 and 2011, according to a new Climate Policy Initiative (CPI) study entitled* ***Deterring Deforestation in the Brazilian Amazon****. The total deforestation registered in that period was 41,500 km - 59% less than would have occurred if deforestation* ***command and control policies*** *had not been changed. (Emphasis added).*[12]

The modernization of the assets related to C2 structures brought with it the migration of a variety of systems to computerized ones. Its current feature is the use of vast computer networks, providing significant gains in terms of speed and volume of information processed and expanded C2 capabilities.

[11] Retrieved from: <http://www.nato.int/cps/en/natohq/topics_69332.htm?selectedLocale=en>. Accessed: 3 February 2016.

[12] Retrieved from <http://climatepolicyinitiative.org/press-release/politicas-de-comando-e-controle-no-brasil-evitam-mais-de-59-500-km2-de-desmatamento-na-amazonia/>. Accessed: November 2, 2015.

4. C2, Network Centric Warfare and Cyberwar

The new conception of computerized C2 military structures led to the concept of NCW, or Network Centric Warfare (NCW), which originated in 1996, when Admiral William Owens of the US Navy introduced the concept in an article for the Strategic Forum, published by the Institute for National Strategic Studies in the USA. The article describes the evolution of C2 and Intelligence systems and their enhanced ability to achieve situational awareness (OWENS, 1996).

The definition of NCW is based on the adoption of a new philosophy focused on combat power. This attribute can be created by establishing an effective link between combat, combat support, and logistics support with dispersed forces within a theatre of operations. These factors made it possible to increase the sharing of situational awareness on the battlefield (ALBERTS, GARSTKA; STEIN, 2000). NCW aims to achieve higher information superiority in relation to the opponent or opponents. According to US manual *JP 3-13: Joint Doctrine for Information Operations*, information superiority is the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

The objective of NCW is to consolidate all the advancements made so far, providing C2 systems at all levels with unprecedented situational awareness (PINHEIRO, 2008, p. 8). The NCW processes should, for example, allow the capture of unmanned aircraft imagery, adding data provided by aerial observers or other sensors and send it to a combat unit that can exploit the information, as in the case of Operation Afghanistan mentioned above.

The main advantages of NCW are, according to Souza (2010): shared situational awareness, rapid decision-making and operations, increased lethality and protection of conventional forces, and maximum synchronization of actions. To achieve these benefits, the principles of NCW must be followed, in particular the interconnection of military networks. One of the features of those networks is increased speed in comparison to traditional ways of communication (SOUZA, 2010). In modern combat, the C2 of an organization must be capable to integrate new NCW ideas in order to improve efficiency.

Despite the NCW definitions presented, mainly from Alberts and Hayes' (2006) perspective, Smith (2010) has a counterargument: he acknowledges the advantages of NCW, but argues that, regardless of how adept institutions may become at optimising this advantage, opponents will always be capable of adapting and understanding its vulnerabilities. The author is evoking the early definitions of C2 in stating that 'rather than optimising a force for NCW, [...] greater emphasis [should be given] to the selection and education of future [...] commanders (SMITH, 2010, p. 68).

The fact remains that the dissemination of NCW concepts, which shows that C2 has become modernised, brought a new concept to the stage: that of Cyber W. One of the first definitions of Cyber W describes it as the offensive and defensive use of information and information systems to deny, exploit, corrupt or destroy the opponent's information-based

values, information systems and computer networks (CAMPER; DEARTH; GOODDEN, 1996). Another definition describes current Cyber W as:

> *Actions by nation-states and non-state actors employing cyber weapons to penetrate computers or networks for the purpose of inserting, corrupting, and/or falsifying data; disrupting or damaging a computer or network device; or inflicting damage and/or disruption to computer control systems (KREPINEVICH, 2012, p. 8, tradução nossa).*

It should be noted that the use of Cyber W can counteract the operation of C2 systems, as these are intrinsically linked and are dependent on computer systems such as NCW systems, which will thus be exposed to that threat. In addition to these traditionally military systems, Cyber W entails the ability to operate across the cyberspace environment, including the Internet, and is thus able to affect ordinary citizens and other institutions. These arguments are supported by the following quote from two Chinese military officers:

> *We can say with certainty that this* ***is the most important revolution in the history of technology****. Its revolutionary significance is not merely in that it is a brand new technology itself, but more in that it is a kind of bonding agent which* ***can lightly penetrate the layers of barriers between technologies and link various technologies which appear to be totally unrelated****. (LIANG; XIANGSUI, 1999, p. 10, emphasis added).*

The increase in the number of Internet users since network access became commercially available in 1995 gave it the status of a global public service (BLUMENTHAL; CLARK, 2009, p 207) and since then it is considered the essential tool of modern society and of the globalised world (KURBALIJA; GELBSTEIN, 2005, p. 7; ZUKANG, 2007, p. 6). However, Cepik et. al. (2014, p. 1) point out that, as society's dependence on computer and computer systems grows, the discussion on the challenges that the digital age poses to national and international security is intensifying.

C2 systems are increasingly present in basic services, which were left vulnerable by the emergence of Cyber W. By extrapolating these findings, one can imagine the urban chaos that a cyberattack could create in a big city, should any of these services be disrupted. In this context, it can be said that a teenager 'armed' with a laptop, with advanced knowledge in cybernetics, could trigger an attack and thus become a type of threat.

The creation of cyberspace brought with it a new form of power. Non-state actors, such as Anonymous and Wiki-leaks, have the capacity to threaten States because they have the ability to interfere in NCW systems, break into government systems, including C2 centres, and expose sensitive information, potentially causing discomfort and even destabilising governments. In the face of the threats posed by both new and old actors, States began to develop cyber defence centres[13], which are now also able act offensively, or preventively, as demonstrated by the following quote:

[13] The Brazilian Cyber Defence Command was activated in 2015.

> **It is no secret that governments are able to intercept telephone calls and text messages**. Today, several companies already provide programs to the government capable of invading your computer, using your webcam, reading your emails, copying documents, of doing whatever they please without being detected', said researcher and American Civil Liberties Union cyber activist Christopher Soghoian (BRASIL, 2014d, p. 7).

It is worth mentioning the example of the actions of North American computer analyst Edward Snowden, who exposed the details of various programs integrated in the global surveillance system of the US National Security Agency (NSA), creating problems between the US government and the governments of Brazil and Germany[14], among other countries. This was a scenario in which 'no one was safe, not even leaders of friendly nations, as was proved' (BRASIL, 2014d, p. 7).

By analysing this approach through the lens of armed conflict and add it to the facts already presented on public opinion, new options for achieving victory came 'and it all these make people believe that the best way to achieve victory is to control, not to kill' (LIANG; XIANGSUI, 1999, p. 27).

To put the potential of this threat into context, in 1997, the US Department of Defence commissioned an experiment codenamed 'Eligible Receiver'. The main objective of the exercise was to see if a group of hackers could infiltrate the Pentagon's computers and gain access to its defence systems:

> *According to then Deputy Secretary of Defence John Hamre, it took three days for someone in the Pentagon to realise that the computer systems were under attack.* **The hackers gained control of the Pentagon and of the military command and control systems**. *A real attack could have shut down the systems. Even more uncomfortable was the thought that the attackers could have gained access and stolen information.* A year later, a real cyber attack was launched against computers in the Pentagon, in the National Aeronautics and Space Administration (NASA) and in other government agencies. The attack was discovered by accident in 2000 and likely originated in Russia (BRASIL, 2011b, p. 88, grifo nosso).

In another example, a computer virus called Stuxnet was created in 2010 which invaded nuclear power systems in several countries, such as India and Iran, and sabotaged their projects. Raphael Mandarino, Director of the Department of Information and Communication Security, Institutional Security Cabinet of the Presidency of the Republic of Brazil in 2011, believed the world was witnessing a well-prepared digital military armament with well-

[14] Snowden revealed that the US government was conducting government espionage, including illegal wiretapping on presidential communications with Brazil and Germany, among other countries. Retrieved from < http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>, <https://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?tid=pm_politics_pop>. Accessed: 21 February 2016.

defined goals[15]. In another case, Clarke and Knake (2015) describe Israel's bombing of the future location for a nuclear facility in Syria. In short, Cepik et. al. (2014, p. 9) claim that Israeli hackers disrupted the Syrian radar system, making Israeli fighters invisible to the enemy air force.

Reinforcing the impact of Cyber W, a study published by the Institute for Applied Economic Research (IPEA) posits that some countries are engaged in a 'Cyber Cold War'. To support this claim, the study cited the issue of the theft of the projects of US fighters by China (MCCAUL, LIPINSKI, 2012) and the industrial sabotage of Iran's nuclear facilities attributed to the US government, in which the Iranian uranium enrichment plant was compromised by means of a computer virus (SANGER, 2012).

The evolution of C2 systems involved increased computerisation due to the generalised use of computer networks and internet connections. The dilemma here presented is that the larger these networks are, the greater the risks posed by the presence of new power players, that is, hackers. Thus, according to Mandarino, Cyber Defence has become a key activity for the security of States (BRASIL, 2013b, p. 17) and for the success of military operations at all levels of command, as they enable C2 by protecting information assets (BRASIL, 2014a, p. 4-8 - 4-9).

5. Conclusion

In our analysis of command and control up to this point, we presented a variety of definitions to acclimate the reader to the subject. It was found that, although the term is generally unknown, activities related to command and control date back to the early days of warfighting.

Currently, the importance of C2 is reflected on how pervasive it has become in current warfare and in the everyday life of cities and people. Perhaps due to the global dissemination of C2 assets through modern communications devices, combined with the growing computerisation of these devices in large conglomerates of networks such as those designed for NCW, new vulnerabilities have been discovered that could endanger citizens, institutions and even States and their foreign affairs.

We were thus able to verify that the developments in C2 had an impact on the defence of nations, as well as observe the changes in warfare that ensued. Finally, in the twenty-first century, the importance of technology and the use of cyberspace is clearly on the rise. Therefore, these issues increasingly occupy the national and international security agenda.

[15] Retrieved from <http://g1.globo.com/tecnologia/noticia/2011/04/stuxnet-poderia-ser-usado-como-arma-militar-diz-chefe-de-seguranca.html>. Accessed: 21 February 2016.

Works Cited

Afonso, S. M.; da Silva, A. S. Comando e Controle: a ótica da defesa social. *Tecnologia & Defesa - Segurança*, v. 8, 2013.

Alberts, D. S. Network Enabled Command and Control: Module 1. **Department of Defense - *The Command and Control Research Program*,** 2009. Retrieved from: <http://www.dodccrp.org/html4/education_main.html>. Accessed: 24 Feb. 2016.

Alberts, D. S.; Garstka, J. J.; Stein, F. P. *NETWORK CENTRIC WARFARE*: Developing and leveraging Information Superiority. Department of Defense - Command and Control Research Program, 2000. ISSN 1-57906-019-6. Retrieved from: <http://www.dodccrp.org/files/Alberts_NCW.pdf>. Accessed: 19 Nov. 2015.

Alberts, D. S.; Hayes, R. E. Understanding command and control. *Department of Defense - Command and Control Research Program*, 2006. Retrieved from: <http://www.dodccrp.org/>. Accessed: 19 Nov. 2015.

Bahmanyar, M. *Afeganistan Cave Complexes 1979-2004* - Mountains strongholds of the Mujahideen, Taliban and Al Qaeda. Oxford: Osprey Publishing, 2004.

Blumenthal S. M., Clark, D. D. *The Future of the Internet and Cyberpower*, 2009. Retrieved from <http://ctnsp.dodlive.mil/files/2014/03 /Cyberpower-I-Chap-08.pdf>. Accessed 13 May 2016.

Boot, M. The new America Way of War. *Foreign Affairs*, v. 82, n. 4, jul./aug. 2003.

Bose, P. *Alexandre, o grande***:** a arte da estratégia. Rio de Janeiro: Best seller, 2006.

Boyd, J. *A discourse on winning and losing. Maxwell Air Force Base***.** Air University Library, 1987.

Brasil. Exército Brasileiro. Manual de Campanha C11-1 - *Emprego das Comunicações*. 2. ed. Brasília, 1997.

Brasil. Manual de Campanha C20-1 - *Glossário de termos e expressões para uso no Exército*. 3. ed. Brasília, 2003.

Brasil. Manual de Campanha C100-5 - *Operações*. 3. ed. Brasília, 1997a.

Brasil. Manual de Campanha EB20-MC10.205 - *Comando e Controle*. Brasília, 2015.

Brasil. Manual de Campanha EB20-MC-10.213 - *Operações de Informação*. Brasília, 2014a.

Brasil. Ministério da Defesa. MD30-M-01 - **Doutrina de Operações Conjuntas** - 2º Volume. Brasília, 2011a.

Brasil. MD31-M-03 - *Doutrina para o Sistema Militar de Comando e Controle*. Brasília, 2014b.

Brasil. Presidência da República. Secretaria de Assuntos Estratégicos. *Desafios estratégicos para a segurança e defesa cibernética*. Brasília, 2011b.

Brasil. Senado Federal. *Em discussão*, a. 5, n. 21, jul. 2014d.

Brasil. Tribunal de Contas da União. *Revista do TCU*, n. 128, 2013b.

Camper, A. D.; Dearth, D. H.; Goodden, R. T. *Cyberwar: security, strategy and conflict in the information age*. 3. ed. Afcea, 1996.

Carrera, I. Por que Alan Turing Influenciou sua vida sem você sequer notar. *Época*, 30 Jan. 2015. Retrieved from: <http://epoca.globo.com/ ideias/noticia/2015/01/bpor-que-alan-turing-influenciou-sua-vidab-sem-voce-sequer-notar.html>. Accessed: 21 Nov. 2015.

Cepik, M.; Canabarro, D. R.; Borne, T. *A securitização do ciberespaço e o terrorismo***:** uma abordagem crítica. Brasília: IPEA, 2014.

Clarke, R. A.; Knake, R. K. *Guerra cibernética:* A próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: BRASPORT, 2015.

Cordeiro, S. S. *A influência da Guerra Cibernética nos sistemas de comando e controle nas operações militares* - Dissertação de Mestrado. Escola de Comando e Estado Maior do Exército, Rio de Janeiro, 2014.

Correia, S. S. *Jornal Opção*, 2014. Retrieved from: <http://www. jornalopcao. com.br/posts/opcao-cultural/guerra-do-paraguai-uma-batalha-que-sera-sempre-maldita-mas-o-brasil-nao-e-vilao>. Accessed: 18 Nov. 2015.

Dempsey, M. E. Win, Learn, Adapt, Win Again. *Armor - Mounted Maneuver Journal,* sep./oct. 2011.

Doratioto, F. *Maldita Guerra*: nova história da Guerra do Paraguai. São Paulo: Companhia das Letras, 2002.

Fonseca, J. J. S. D. *Metodologia da pesquisa científica*. Fortaleza: Editora da UECE, 2002.

Ford, D. *A vision so noble:* John Bold, the OODA Loop, and the America's War on Terror. New Hampshire, USA, 2010.

Hodges, A. *Alan Turing:* The enigma. Princeton University, 2014.

House, J. M. Toward combined arms warfare: A survey of 20th century tactics, doctrine and organization. *Combat Studies Institute, US Army Command & General Staff College Press*, Fort Leavenworth, 1984.

Hughes, D. J. *Moltke on the Art of War*. New York: Presidio Press Book, 1993.

Jomini, A. H. D. *The art of war (1836)*. Rockville: ARC Manor, 2007.

Krepinevich, A. F. *Cyber warfare:* a "nuclear option"? Washington: Center of Strategic and Budgetary Assessments, 2012.

Kurbalija, J.; Gelbstein, E. *Gobernanza de Internet:* Asuntos, Actores y Brechas. DiploFoundation, 2005.

Lele, A. Operation Neptune Spear and Role of Technology. *Journal of Defence Studies,* v. 5, n. 4, oct. 2011.

Liang, Q.; Xiangsui, W. *Unrestricted warfare*. Beijing: PLA, 1999.

Luddy, J. *The challenge and promise of network-centric warfare*. Arlington: Lexington Institute, 2005.

Mccaul, M.; Lipinski, D. *Congressman Daniel Lipinski*, 2012. Retrieved from: <https://lipinski.house.gov/press-releases/house-passes-lipinskimccaul-cybersecurity-enhancement-act-to-secure-federal-networks-critical-infrastructure-and-americas-competitive-edge/>. Accessed: 25 Feb. 2016.

Magnoli, D. *História das Guerras*. São Paulo: Contexto, 2006.

Orr, G. E. *Combat Operations C3I - Fundamentals and Interactions*. Alabama: Air University Press, 1983.

Owens, W. A. The emerging U.S. system-of-systems. *Strategic Forum*, n. 63, feb. 1996.

Pearson, D. E. *The World Wide Military Command and Control System*: evolution and effectiveness. Alabama: Air University, 2000.

Pinheiro, Á. D. S. A tecnologia da informação e a ameaça cibernética na guerra irregular do século XXI. *PADECEME*, n. 18, p. 4-11, mai./ago. 2008.

Portugal. Ministério da Defesa Nacional. Exército Português. *A guerra do Golfo de 1991*. Lisboa,, 2008.

Portugal. Estado Maior do Exército. *PDE-3-00 - Operações*. Lisboa, 2012.

Portugal. Comando e Controlo na Artilharia Antiaérea. *Boletim da Artilharia Antiaérea,* n. 14, out. 2014.

Raugh, D. L. Organizing a tank battalion for the counterinsurgency fight: A study in organization design armor. *Mounted Maneuver Journal*, may/jun. 2011.

Sanger, D. E. Obama order sped up wave of cyberattacks against Iran. *The New York Times,* 2012. Retrieved from: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0>. Accessed: 14 May 2016.

Schermerhorn, J. *Administração*: conceitos fundamentais. Rio de Janeiro: LTC, 2006.

Schlosser, E. *Comando e controle*: Armas nucleares, o acidente de Damasco e a ilusão de segurança. [S.l.]: Companhia das Letras, 2015.

Smith, C. R. *Network Centric Warfare, Command, and Nature of War*. [S.l.]: Canberra, 2010.

Souza, C. R. P. D. *Sistema Integrado de Monitoramento de Fronteiras (SISFRON)*: concepção estratégica e estrutura. Rio de Janeiro: Escola de Comando e Estado Maior do Exército, 2010.

Sproles, N. *Establishing Measures of Effectiveness for Command and Control:* A System Engineering Perspective. Department of Defense - Defense Science & Technology Organization, 2001.

USA. Report to the Congress of the United States. *World Wide Military Command and Control System*. Washington: General Accounting Office, 1979.

USA. The U.S. Department of the Navy. *MCDP-6. Command and Control*. Washington, 1996.

USA. The U.S. Department of the Army. *FM 1-02. Operational Terms and Graphics*. Washington, 2004.

USA. *FM 3-0. Operations*. Washington, 2008.

USA. The U.S. Department of Defense. *The Dictionary of Military Terms*. Washington, 2009.

USA. U.S. Army. *War in the Persian Gulf*: Operation Desert Shield and Desert Storm - August 1990 - March 1991. Washington: Center of the Military Story, 2010.

Van Creveld, M. *Command in war*. Cambridge: Harvard university Press, 1985.

Weatherford, J. M. *Gengis Kahn e a formação do mundo moderno*. Rio de Janeiro: Bertrand, 2010.

Yarmie, M. S. The communications bridge: planning and implementing strategic communications for enduring freedom and beyond. *U.S. Army War College*, 2003.

Young, R. 21st Centuryer Development: Understanding what is in the Tool Bag. Armor. *Mounted Maneuver Journal*, 2011.