

Evaluating Command and Control Systems' Effectiveness in Enhancing Situational Awareness: ENDF 6th Mechanized Division in the Danakil Desert.

¹Col Amanu Megersa Kicha, ²Dr Zedekiah Sidha & ²Colonel (Dr) John R Kisilu

¹Ethiopian National Defense Force

²National Defence University-Kenya

DOI: <https://dx.doi.org/10.47772/IJRISS.2024.8080150>

Received: 13 July 2024; Revised: 04 August 2024; Accepted: 06 August 2024; Published: 07 September 2024

ABSTRACT

Effective military command and control is critical for the success of modern military operations. C2 systems enable the coordination of forces, decision-making, and information sharing across hierarchical command structures. This paper provides an overview of C2 key concepts and challenges in military C2. It examines the evolution of C2 approaches from centralized to more distributed models, driven by factors such as technological advancements, the complexity of the battle space, and the need for adaptability. The paper discusses the role of information systems, situational awareness and risk assessment, communication networks, decision support tools in enhancing C2 capabilities. It also highlights issues around interpretability, resilience, and the integration of emerging technologies like artificial intelligence and the role of all level military commanders. The analysis draws on case studies and empirical research to identify best practices and areas for further improvement in military C2. The findings aim to inform military leaders, policy makers, and system designers on strategies to strengthen command and control for future military operations.

Keywords: Command and Control, Danakil desert, Field manual, Joint operation, and military operation.

INTRODUCTION

Command and control is a "set of organizational and technical attributes and processes that employs human, physical, and information resources to solve problems and accomplish missions" to achieve the goals of an organization or enterprise, according to Marius Vassiliou (2015), definition by military scientists. A NATO (1988) definition is that command and control is the exercise of authority and direction by a properly designated individual over assigned resources in the accomplishment of a common goal. Military command and control (C2) is a critical function that enables armed forces to plan, coordinate, and execute operations effectively. The command and control structure provides the framework for military leadership to direct the activities of subordinate forces, share information, make decisions, and respond to evolving situations. Effective C2 is essential for achieving military objectives, maintaining situational awareness, and ensuring the optimal employment of available resources.

In modern warfare, the complexity of operations, the proliferation of information systems, and the need for joint and multinational coordination have heightened the importance of robust and resilient command and control capabilities. Military organizations must continuously adapt their C2 structures and processes to keep pace with technological advancements, changing strategic environments, and emerging threats. This journal article aims to explore the fundamental aspects of military command and control, key principles, organizational structures, and the ongoing challenges faced by defence establishments in maintaining effective C2 in a dynamic and rapidly evolving operational landscape. By examining both the theoretical underpinnings and practical applications of military C2, this study seeks to contribute to the broader understanding of this critical domain

and inform discussions on the future development of command and control systems.

The article will delve into topics such as the C2 structure, communication networks, situational awareness and risk assessment, decision-making frameworks, intelligence integration, information management, command and control in joint operation, command and control in cyber operation, and resilience of military command and control. Additionally, it will analyze the implications of factors such as organizational culture, leadership, and interoperability on the effective implementation of C2 practices. Through a comprehensive review of the existing literature and case studies, this journal article will provide readers with a detailed examination of the fundamental principles, challenges, and best practices in military command and control, in ENDF 6th Mechanized Division in the Danakil Desert with the aim of informing both academic discourse and practical applications in the field of defense and security.

THEORETICAL FRAMEWORK

Theoretical frameworks are essential for succinctly outlining the fundamental concepts that define the discussed issues. They also outline the areas of knowledge considered in the research effort, indicating the theoretical assumptions of the study and providing a clear framework for the scope and objectives within academia. The following theory guided the study.

The term military leadership refers to processes of influence and command in connection with the military and warfare. The specificity of military leadership results from the dense intertwining of these processes with the violent character and the hierarchical structure of the military organization. The military hierarchy is a one-dimensional concept of leadership: Social influence on the behavior of people is exerted by a single person at the top of the hierarchy who is able to steer the thoughts, feelings, and actions of subordinates through his or her words and deeds; his or her orders are translated directly into military actions. A chain of command and command structure enables social influence to move from top to bottom by means of a chain of command and to reach all levels of the (Holenweger, 2023)

The theoretical framework would evaluate how the Ethiopian national defence 6th mechanized division command and control systems enable to the achievement of situational awareness in the challenging Danakil desert environments. That includes communication system, decision making of command, alignment between organizational structure, identification of gaps and vulnerabilities. By applying this multi-faceted theoretical

RESEARCH METHODOLOGY

This study adopted an exploratory research design. The an exploratory exploratory study design was chosen because it allows studies to pursue unique and upcoming ideas to to prepare the ground for the collection of new information that can be utilized by future studies in the area. The study was undertaken through a review of existing literature, academic research papers, and publications related to the subject matter. This helped in gaining initial insights, identifying gaps, and finetuning the research question. Secondary data was collected from reliable and reputable sources relevant to the research objectives. Official report/documents, peer reviewed journal articles and published dissertations.

FINDINGS

In desert operation the command and control needs integration of advanced sensor systems, data fusion algorithms, and digital mapping tools allowed commanders to maintain a more comprehensive and real-time picture of the operational environment. This enhanced their ability to make informed decisions and direct forces effectively. Robust voice, data, and video communication links between headquarters, maneuver units, and support elements facilitated faster information sharing and improved synchronization of operations. The harsh desert terrain, extreme temperatures, and limited infrastructure in Danakil desert posed significant challenges to maintaining reliable connectivity and uninterrupted command and control. Workarounds and redundant systems were required to mitigate these issues. The exercise highlighted desert warfare training and the refinement of command and control doctrine to optimize procedures for operating in such environments.

As the experience of the US army command and control in desert operation shows the first challenge was communication challenges which include extreme heat, dust, and vast distances in desert environments posed significant challenges for reliable communications. Moreover environmental challenges were expressed in terms of extreme temperatures, limited water resources, and lack of cover and concealment in desert environments required specialized training and equipment. Therefore, these findings highlight the unique challenges faced by the US army in maintaining effective command and control during desert operations and the need for specialized capabilities and adaptations to succeed in such environments is also seen in my research findings in Ethiopian Danakil desert command and control operations.

The 6th Mechanized Division in Danakil desert operation involves military operations based on their mission in desert environments. These operations require specifically trained personnel and specialized equipment to navigate and operate effectively in these harsh conditions. Command and control are crucial to any military operation, including those in the desert. Command and control refers to planning, directing, coordinating, and controlling military forces during operations. In Danakil desert operations, command and control become even more vital due to the unique challenges posed by the environment. One of the key aspects of command and control in a desert operation is ensuring a clear communication network. This is necessary to enable information sharing among different combatant units and to maintain situational awareness. Danakil deserts often have vast, open spaces with limited or no natural cover, hindering communication. Therefore, establishing reliable and secure communication channels, such as radio systems networks, is crucial.

DISCUSSIONS

Command and control system

Understanding Command and Control C2 is no longer an option; it is a requirement. Significant progress on Defense transformation or success in 21st century operations, we need to understand Command and Control thoroughly. This article is intended to provide a sound foundation for efforts to better understand Command and Control. The mission challenges of the 21st century have increased significantly. Fortunately, new concepts of operations and approaches to Command and Control are able to provide significantly increased capabilities to deal with these challenges (Alberts, 2006). The mission challenges of the 21st century have increased significantly. Fortunately, new concepts of operations and approaches to Command and Control are able to provide significantly increased capabilities to deal with these challenges.

As Alberts (2006) explained about command and control the today's missions differ from traditional military missions, not just at the margins, but qualitatively. Today's missions are simultaneously more complex and more dynamic, requiring the collective capabilities and efforts of many organizations in order to succeed. This requirement for assembling a diverse set command and control. Understanding command and control importance of understanding C2 of capabilities and organizations into an effective coalition is accompanied by shrinking windows of response opportunity. Traditional approaches to Command and Control are not up to the challenge. Simply stated, they lack the agility required in the 21st century.

Experience of US Army Command and Control in Desert Operation

According to Major Michael and R. Macedonia (1992), explained about US army experience during operations Desert Shield and Desert Storm communications were critical to controlling the scope of operations. During these operations command and control experiences in desert operation, that the US army faced challenges with coordinating large scale troop movements and logistics through the vast and featureless desert terrain. Effective satellite communications and GPS were critical for navigation and situational awareness. The army relied heavily on air power and advanced technology like Patriot missile defense systems to offset the Iraqi army's numerical advantages. Effective integration and coordination between ground force, air support and intelligence assets was essential for the coalition decisive victory.

US Iraq war (2003-2011) urban combat in cities like Fallujah presented challenges for army command and control requiring flexible and decentralized operations by small units. Roadside bombs and insurgent attacks

distributed communication networks and made it difficult to maintain a common operational picture. The army utilized advanced unmanned aerial vehicles. Signal intelligence and biometric databases to enhance intelligence gathering and targeting of insurgents. Interoperability between the army, coalition partners, and Iraqi security forces was an ongoing challenge that impacted coordination and information sharing.

US Department of the Army (1993) indicated that the primary challenges encountered in desert warfare stem from extreme heat and scarcity of moisture, influencing the tactics, techniques, and procedures employed. Desert warfare refers to military operations conducted in desert or comparable arid or semi-arid regions. This term encompasses military activities influenced by such areas' unique training, climate, resource availability, and the strategies and tactics employed by military forces operating within these challenging environments.

Generally, the desert environment has necessitated the US army to develop robust, networked and adaptable command and control capabilities to achieve battlefield dominance. Key lessons include the critical roles of communications, intelligence, air support integration, and multinational coordination.

Command and Control system in 6th Mechanized division

For the purpose of communication commanders must use advanced maps, satellite imagery, and other geospatial tools to understand the terrain, identify potential obstacles, and develop effective routing and maneuver plans. In the 6th division maintaining situational awareness is another crucial aspect of command and control in Danakil desert operations. This involves continuously monitoring the battlefield, tracking the movement of friendly and enemy forces, and assessing the overall operational picture. This information is vital in decision-making, enabling commanders to adjust their plans, allocate resources, and coordinate forces accordingly. Command and control in Danakil desert operations emphasizes the effective use of combined arms tactics.

Command and Control structure

The concepts of mission command date back to the 1890s when Prussian-German tacticians, unhappy with overly directive types of command, developed a more flexible construct called Auftragstaktik, which empowered subordinate commanders to exercise initiative. The United States Army Functional Concept for Mission Command, "translates roughly to mission-type tactics" and essentially "held each German commissioned and noncommissioned officer duty bound to do whatever the situation required, as he personally saw it." This concept was vital in allowing subordinates to exercise judgment and initiative in an operational environment characterized by slow communications a place where a "decentralized approach to or Auftragstaktik, proved more effective than a highly centralized command (Carpenter, 2016).

The US Department of Defense Dictionary of Military and Associated Terms defines command and control as: "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission". Command and control (C2) structure refers to the system and processes through which an organization, typically a military or a business, exercises direction, coordination, and control over its resources and activities. In a military context, C2 structure involves the allocation of responsibilities, decision-making processes, communication systems, and operational procedures to effectively command and control forces during missions. In a business context, C2 structure involves the allocation of responsibilities, decision-making processes, and communication channels to ensure effective management and coordination of activities within the organization.

As Ramezanale (2011) explained the levels of commanders, it is possible to classify the available information and decision making levels of command and control centers in military field. Creating strategic, tactical, and operational command and control centers is for the same reason. For example, a command and control center in strategic level of military field would be a place for determining master strategies and priorities, planning master plans and strategic guidance which is effective for massive orientation, and developing foreign policies in any country. Strategic planners just focus on making use of specific military resources in order to achieve to their political purposes. Therefore, it is necessary to have a complete set of tools and instruments provided for strategic goals to gain the ascendancy over the enemy. Operational information can be a part of these tools. This kind of separation of powers can also be true in the field of crisis management because the total issue is the same and

only the details of programs, methods of performance and the performers might be different.

In the field of crisis management, managers of the strategic level can develop a strategic map and make organizational master decisions and this process would take days and weeks in case of normal conditions.

Operational level which basically focuses on response operation in disaster area is depended on direct observation and quick decision making with assistance of knowledge extracted from available information. Tactical level managers mainly focus on coordination of organizations and their activities. Providing and procurement of needed resources for normal or critical conditions, creating inside and outside organization coordination procedures, enhancing capacities and capabilities of organizational subunits and collection of information for strategic level will be the most important measures of the tactical level (Ramezani, 2011).

As US field manual 7-100.1 explained about the structure of C2 at each level of command is very similar, designed with the same basic structure and emphasis on survivability through mobility, redundancy, and security. The higher the level of command the larger and more complex the staffs. Supporting each staff is a series of multiple command positions and communications systems, providing the flexibility required on a highly fluid, lethal battlefield. The professional training of commanders and staffs emphasizes consistency in staff planning procedures at all levels of command. Emphasis on responsive planning (assisted by automation) in the C2 process has produced a cadre of professional, highly-trained staff officers. Thoroughly educated in all aspects of strategy, operations, and tactics, these officers are capable of functioning from the General Staff down to tactical level. Operational commanders must be equipped to control the full scope of combined arms, joint, interagency, and multinational activity.

The Ethiopian national defence forces is the military of Ethiopia, composed of the ground force, air force and specialized forces. The overall command and control of the Ethiopian defence force is centralized under the Ethiopian ministry of defence forces. At the highest level Ethiopian national defence force is led by commander in chief, who is the prime minister of Ethiopia. Under ground force army then division. 6th Mechanized division is one of mechanized division deployed in Danakil desert.

Communication network

A command, control, and communication C3 system is an information system employed within a military organization. It is a general phrase that incorporates strategic and tactical systems. Consequently, a combat direction system, tactical data system, or warning and control system may each be considered C3 systems. Throughout this text, attention has been directed toward principles and technologies associated with the hardware of weapons systems. Underlying these weapons systems and the methods by which they are caused to function, is the fundamental concept that they are simply devices or processes that serve as tools to augment the capabilities of a human being. For example, an electromagnetic sensor may augment the visual and audio sensor of an individual; a weapon enhances the individual's ability to inflict damage; a combat direction system expands the decision making capacity of a person; and so forth. At the functional center, no matter how remote, of every weapon system, combat system, or combat direction system is a human being who is engaged in the employment of that system or grouping of systems.

As United States Naval Academy Weapons and Systems Engineering Department explained that digital communications between computers allows much more rapid exchange of data than would be possible using human language. Indeed, it is the only ways that complete information can be made available to all involved in the decision-making process. In order for all services and agencies, including those from allied countries, to mutually support one another, a series of data-link standards have been agreed upon that apply to all systems and are implemented regardless of the communications method employed. A series of standard formatted messages are used to exchange digital data between the computers associated with the systems. These messages contain the various elements of information required for digital exchanges. The messages are interpreted by the computers and converted into display information for use by systems operators.

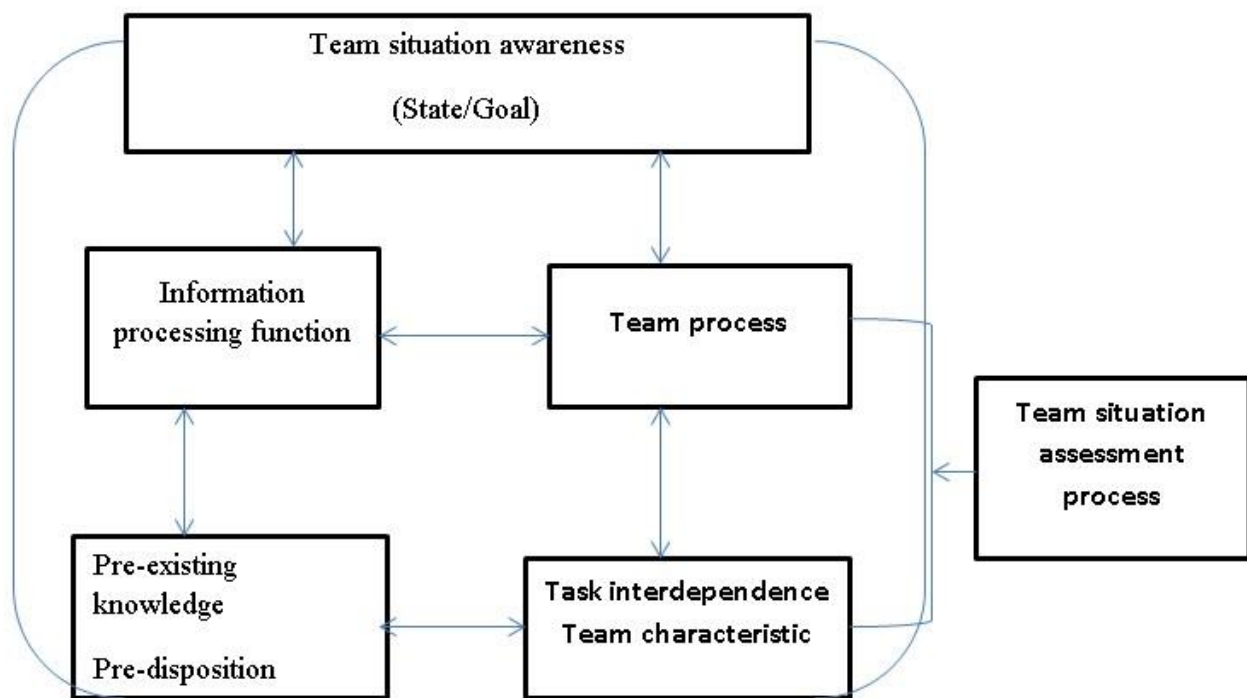
In mission of 6th mechanized division Danakil desert areas' vast and open nature can hinder communication and result in limited or disrupted connectivity. The areal storms can also damage equipment and compromise the

functioning of sensitive electronic communication systems. Also, the scorching heat in the area limits communication signals compared with other regions.

Situational awareness and risk assessment

As McNealy (1999) cited in Sonnenwald and Pierce (1996) explore the relationship between changing battlefield requirements and organizational design, with a focus on how the social network and information flow affect situational awareness. In their findings they identified a group, or team, situational awareness as facilitating task completion. Additionally, they discussed the critical nature of situational awareness and how it can provide for smooth operation center shift changeovers. A shift changeover, in broad terms, is the transference of the current situational awareness from one group to another, which will then be expected to maintain the situational awareness in the same manner. Issues of trust in the subordinates or peers who will accept the transference become paramount. Sonnenwald and Pierce report that an “iron man” culture has evolved in which the superiors stay awake during an entire operation’s duration because they fear their expertise and grasp on the current situational awareness cannot be replaced or duplicated.

Building on the individual situational awareness conceptualization, they produced a conceptualization of team situation awareness that consists of the interaction of the individual’s situational awareness with the team functions and characteristics. The next figure is conceptualization of team situation awareness.



Source: McNealy 1999

Team Situation Assessment (Process) 12 functions and then interacts with the end-state, or goal, of situation awareness. In the team situational awareness model, the team processes and characteristics interact, positively or negatively, with the individual’s situational awareness. However, they have not extended this model to include a larger team comprised of multiple subgroups (McNealy, 1999).

As McNealy (1999) explore the relationship between changing battlefield requirements and organizational design, with a focus on how the social network and information flow affect situational awareness. In their findings they identified a group, or team, situational awareness as facilitating task completion. Additionally, they discussed the critical nature of situational awareness and how it can provide for smooth operation center shift changeovers. A shift changeover, in broad terms, is the transference of the current situational awareness from one group to another, which will then be expected to maintain the situational awareness in the same manner. Issues of trust in the subordinates or peers who will accept the transference become paramount.

In Danakil 6th mechanized Division maintaining situational awareness is another crucial aspect of command and control in desert operations. This involves continuously monitoring the battlefield, tracking the movement of friendly and enemy forces, and assessing the overall operational picture. This information is vital in decision-making, enabling commanders to adjust their plans, allocate resources, and coordinate forces accordingly.

Additionally, command and control in desert operations emphasizes the effective use of combined arms tactics. Desert environments demand a combination of infantry, armor, artillery, and air support to overcome the challenges posed by the terrain and the enemy. Commanders must integrate these different elements and coordinate their actions to achieve synchronized and complementary effects on the battlefield.

Situational awareness and Risk assessment in 6th Mechanized division

The mission area of 6th mechanized division the Danakil desert terrain often consists of dunes, rocky terrains, and vast open spaces, which can pose challenges for mobility and deployment of forces. The fluid and unpredictable nature of desert environments can make it difficult for commanders to efficiently and rapidly coordinate movements and react to changing situations. Limited visibility: Sandstorms and dust clouds are expected in desert environments, severely limiting visibility. This makes it challenging for commanders to gather real-time intelligence, monitor the battlefield, and make informed decisions. Camouflage and concealment: Desert environments offer limited natural cover and concealment, making it challenging to hide troops, vehicles, and equipment from the enemy. Commanders must employ effective camouflage and concealment techniques to avoid detection and maintain the element of surprise.

DECISION MAKING

The activities of the military operation being supported by the system are continuously monitored. Some decision situations are delegated to the routine system operators and others require the guidance of the commanders or their immediate staff.

As US Army (2022) stated the military decision-making process is not a boogeyman to be feared, but a process to be embraced and mastered by all staffs charged with developing operations plans and orders. It is a systematic process that enables commanders and their staffs to apply critical and creative thinking and doctrine to solve problems and establish the framework and conditions for commanders to make effective decisions. And, like everything else in the Army, it requires time and training for staffs to become experts in the process. Observations emanating from the combat training centers and Mission Command Training Program consistently bear out that commanders and staffs are more successful when they have done the hard work of training the in the run-up to their rotation (Army, 2022).

Information Management

As US Military Information Technology Systems Radio array neutron detector was at the forefront of early computer science and information technology innovations, building computers in the 1950s to improve researchers' military modeling capabilities and developing data communications technologies that were the forerunner of the internet. Today, Radio array neutron detector researchers provide evaluations to military leadership and recommend policies and best practices and best practices to support continued technical innovation, adoption, and protection of critical military system.

As Uhm (2011) explained about information, an information operation involves the coordination of activities in the information domain which aim to influence the will, perception and capability of approved target groups. They also involve activities designed to protect our own freedom of movement within the information domain, to protect friendly information and information processes and to aback information and information systems of a potential adversary. This means that information operations do not in theory have their own capacities, but that they are an integral part of all operational activities. The staff may include a section which facilitates the coordination process and supports other sections in information operations.

Public affairs, information and media The public affairs officer, supported by the office Public affairs, advises

the commander on all media-related matters, on the basis of the guidelines in the information strategy formulated at the highest politico-military level. To ensure synergy and unity of opinion, the political authority operation must coordinate closely at all command levels with all other actors in the field of information dissemination and collection, including command and control joint operation. Program assistant activities must also be closely linked to information operations. The Public affairs, information ensures the harmonization of the program assistant elements of other international organizations and actors active in the mission area. The media information center is the interface with the international and local media. The political authority operations formulates the information strategy and supports the implementation; he is also in principle the joint commander's spokesman and, in that capacity, must have direct access to the commander if necessary. Given that the success and credibility of the spokesman depend on constant contact with the press and on mutual trust, a rapid changeover spokespersons should be avoided (Uhm, 2011).

Command and Control in joint operation

As US joint operation (2011) explained joint operation is a general term that describes military actions conducted by joint forces or by Service forces employed under command relationships. The command and control function at the operational level is the most important operations function because it ties together the other functions at all levels of war across the range of military operations. The strategic environment is characterized by uncertainty, complexity, and rapid change, which requires persistent engagement. This environment is fluid, with continually changing alliances, partnerships, and new national and transnational threats constantly appearing and disappearing. In addition to traditional conflicts, to include emerging peer competitors, significant challenges continue to include irregular warfare, catastrophic terrorism employing weapons of mass destruction, and the ability to project power and maintain its qualitative superiority.

Functions those are common to joint operations at all levels of war fall into six basic groups command and control, intelligence, fires, movement and maneuver, protection, and sustainment. The joint functions reinforce and complement one another, and integration across the functions is essential to mission accomplishment. Command and Control encompasses the exercise of authority and direction by a commander over assigned and attached forces to accomplish the mission. The joint force capability is provides operational vision, guidance, and direction to the joint force (USJO, 2011).

Command and Control in Cyber operation

The definition of cyber effect operations is based upon the U.S. intelligence concept of Computer Network Attack. It can be distinguished from Computer Network Exploitation, commonly referred to as cyber espionage. This is not to say NATO members have been inactive in cyberspace altogether. The Cyber Operations Tracker by the Council on Foreign Relations, one of the most comprehensive databases of publicly known state-sponsored cyber activity, attributes a wide number of cyber espionage activities to the intelligence agencies of various NATO countries. However, it only has NATO entries for the United States and the United Kingdom conducting cyber effect operations.

Command and control is a method that cybercriminals use to communicate with compromised devices within a target company's network. In a C2 attack, an attacker uses a server to send commands to and receive data from computers compromised by malware. This server is also known as a C2 server. The attacker can use the server to perform various malicious actions on the target network, such as data discovery, malware spreading, or denial of service attacks. The server can also serve as the headquarters for a botnet, which is a network of infected devices. C&C communication is a critical step in the process of carrying out an attack on a network or offering malicious services to other actors (Bergmans, 2023).

The combatant commands are responsible for maintaining command and control of all forces in their Aerial reconnaissance during military operations, in times of conflict and peace, and during crisis interventions, such as humanitarian relief or disaster response activities. Two critical ingredients to any successful military operation are timely, reliable situational awareness and efficient, secure communication of that information to all participants in the operation. The cyber challenges to the realization of those ingredients fall into two main categories: mitigating difficulties caused by the inability of multiple users to share information over disparate

computing systems and addressing problems caused by either a lack or overabundance of data relayed to combatant commands during operations (Staheli, 2016)

Today, cyber defense philosophies make little use of military strategy and tactics. Military commanders know that there are times when the best defensive strategy is to take the offensive. They also know the value of the tactics of deception and maneuver. The fact that cyber defense philosophies, such as the defense-in-depth philosophy, do not take advantage of offensive operations, or use the tactics of deception and maneuver, inhibits the defenders from being as effective as the attackers. Current cyber defense strategies tend to be static and their tactics tend to be reactive. The trend is to build layers of static defenses in the hope that every attack will be defeated by at least one of the layers. When this fails, there is a reaction that consists of determining where and how the defenses were penetrated, patching the defenses to stop future similar penetrations, and restoring the system to a coherent state (Howes, 2005).

Challenges of Military Command and Control

Military command and control refers to the exercise of authority and direction by a designed force in the accomplishment of a mission. While modern technology has greatly enhanced military C2 capabilities, there are still several challenges associated with it. Some common challenges of military command and control:-

Information overload: According to Canadian Forces College, there are currently 3.5 billion smartphone users in the world, which equates to 45.04 percent of the world's population. In 2016, that number was only 2.5 billion users, 33.58 percent of the world's population then. The current contemporary operating environment is complex. Conflicts are now fought in five different domains, air, land, sea, cyber, and space. The addition of cyber and space as domains has made the concept of war more complicated, and these new domains are not as well understood. Today's warfighters need situational awareness of all five domains to make the right decision and achieve their missions. Warfighters have mobile battle management systems (BMS) to provide, at the lowest levels, the required SA and improve decision-making. These BMS have various functions such as sending and receiving digital orders, target (Thibodeau, 2020).

Communication and interoperability: - Since the end of the Cold War, interoperability has been at the heart of a debate over the viability and relevance of the NATO Alliance in a new security environment. The shift of focus from territorial defense to multinational expeditionary missions (Afghanistan, Kosovo, Libya) and the challenges encountered executing them has demonstrated the limits of Allied interoperability. While some interoperability challenges (sovereignty concerns, differing national interests, cuts in defense spending, support for local defense industries, and disparities in technological capabilities) can only be resolved by politicians at the strategic level, there are also numerous tactical challenges to interoperability. They include technological disparities, command and control, doctrinal differences, and resource gaps. To mitigate them, Connected Forces Initiative (Derleth, 2015).

Decision making under uncertainty: The military has developed efficient methods for operating in uncertain environments. Armies typically operate in two main modes: risk management in peacetime and uncertainty management in wartime. The two modes enable structure and organisation in times of peace and agility in times of conflict. In peacetime for example, strictly following protocols can keep units safe and organised, avoiding unnecessary injuries or accidents, but while in conflict situations, decision-making is distributed and flexibility is given soldiers to give them agility and effectiveness. Generals are typically managers in peacetime and leaders in wartime. In the uncertainty and messiness of a war zone, they deploy two main methods to operate as smoothly as possible; information-based solutions and action-based solutions (Hilary, 2015).

Hilary (2015) explained that when negative surprises arise, we often dismiss them as 'black swans', freak events that no one could have anticipated. We blame fate for these, and absolve ourselves from our past responsibility. The approach followed by the military suggests that handling uncertainty in a structured framework is crucial to any organisation, insofar as it helps you react quickly and boldly to surprises despite incomplete information. This could be the difference between organisational life and death.

Decentralization and delegation: Decentralized command is a hallmark of the Navy and Marine Corps team. Its

tenets go hand in hand with maneuver warfare, and empowering subordinates to act on commander's intent is the most effective way to weaponize tempo at both the operational and tactical levels. Through numerous conflicts, the sea services have evolved to appreciate the necessity for mission orders and decentralized command. With advances in technology, however, national command authorities now can have an active say in military operations down to the tactical level. There clearly is value in instantaneous communications, but the potential downside is alarming. If a senior civilian or military leader were to lose confidence in a particular plan, operation, or commander, he or she no longer would have to use the chain of command but could reach down directly into the fight in real time and direct forces. This would negate almost 250 years of command evolution (USNI, 2020).

Cyber threats and information warfare: As Smeets (2023) explained the lack of critical attention towards understanding the challenges of developing a military cyber capacity can be attributed to two potential reasons. Firstly, scholarly research has primarily focused on studying the United States and a limited set of other prominent actors, such as Russia, China, North Korea, and Iran, who are extensively engaged in cyberspace activities. Not as much attention is paid to less active militaries. Secondly, investigating the military adaptation of states to the cyber domain necessitates delving into the internal workings of these states, which presents inherent difficulties due to the sensitive nature of such information. This requirement to 'open the black box' and gain insights into internal processes often poses significant challenges.

Training and education: Due to lack of training development resources, the Armed Forces do not have up to date training and education products, the foundation for standard based training and leader development. Standards are the basis for developing training, assessing performance and providing feedback.

In the 6th Mechanized Division the main challenge is the Danakil desert is and extremely harsh, arid, and inhospitable environment, characterized by rugged terrain, extreme heat, and limited infrastructure. This poses significant logistical and operational hurdles. This restricts the ability to rapidly concentrate maneuvers, and maintain cohesion across the mission areas.

Addressing these challenges requires a combination of the technological advancements, organizational structures training and education, and adaptive processes to enhance military command and control capabilities in future operations.

RECOMMENDATION

Depending on discussions on military command and control of 6th mechanized division in Danakil desert the following recommendations are forwarded.

Clear chain of command and decision-making processes is needed - Establishing unambiguous authority structures and communication protocols is crucial for coordinating forces effectively. Military command and control effectiveness thus depends on effective decision making within military command and control systems and structures in all level of commanders.

Analysis of the decision making processes is needed to be employed in joint operations, considering factors such as information sharing, command relations, and the integration of inputs from multiple sources through evaluation with the use of decision support tools, collaborative planning systems, and the role of senior commanders in guiding joint decision-making .

Robust information management and sharing is vital - Efficient gathering, processing, and distribution of real-time intelligence and operational data enables informed decision-making. Resilient communication networks - Redundant and secure communication systems are needed to maintain command and control under diverse conditions.

Technological integration is needed - Leveraging advanced technologies like data analytics, automation, and secure digital infrastructure can enhance responsiveness and decision support. The latest advancements in technologies such as artificial intelligence, machine learning, big data analytics, and network-centric

operations, and their impact on military command and control systems. Thus, employing these systems support military commanders for timely and effectively decision making by predictive analytics, decision support systems, and network resilience.

Familiarizing concerned combatants with joint operation doctrine publications that outline the principles, concepts, and procedures for conducting joint operations is compulsory. Moreover, examining historical and contemporary case studies of joint operations to understand the challenges, successes, and lessons learned in command and control is also needed.

Exploring the command structures employed in joint operations, including the roles and responsibilities of different components land, air, sea, space, and cyber is essential which involves analysing the establishment of joint task forces, combined joint task forces, and examining how these structures facilitate unity of effort and effectiveness of command and control.

Training and rehearsals are needed - Regular exercises to test and refine command and control procedures are important for ensuring preparedness. In each level commanders active military service attending military training courses or workshops that focus on command and control is vital to develop decision making ability that can help in providing insights in to practical applications, case studies, and real-world scenarios.

REFERENCES

1. Staheli, (2016). Cloudbreak: Answering. LINCOLN LABORATORY JOURNAL n VOLUME 22, , 61. chrome-extension://efaidnbmnnnibpcajpcgglefindmkaj/https://www.ll.mit.edu/sites/default/files/publication/doc/cloudbreak-answering-challenges-cyber-command-staheli-109245.pdf
2. Alberts. (2006). Understanding Command and Control. In The futuer of command and control. Washington D.C. chrome-extension://efaidnbmnnnibpcajpcgglefindmkaj/http://www.dodccrp.org/files/Alberts UC2.pdf
3. Army, U. S. (2022). Military decision making process. Center for army lessons learned. chrome-extension://efaidnbmnnnibpcajpcgglefindmkaj/https://api.army.mil/e2/c/downloads/2023/11/17/f7177a3c/23-07-594-military-decision-making-process-nov-23-public.pdf
4. Bergmans. (2023). What are command and control attac? . Command and control definition. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/command-and-control/
5. Carpenter. (2016). Command and Control of Joint Operations Through Mission Command . Air and Space Power chrome-extension://efaidnbmnnnibpcajpcgglefindmkaj/https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-1/2017_1_06_carpenter_seng.pdf
6. Derleth. (2015). Enhancing interoperability. the foundation for effective NATO operations. https://www.nato.int/docu/review/articles/2015/06/16/enhancing-interoperability-the-foundation-for-effective-nato-operations/index.html
7. Hilary. (2015). Eight Ways the Military Manages Uncertainty. https://knowledge.insead.edu/strategy/eight-ways-military-manages-uncertainty
8. Holenweger, M. (2023). Military Leadership: Concepts and Theoretical Approaches.
9. Howes, M. a. (2005). On Cyber Warfare Command and Control Systems . 05. chrome-extension://efaidnbmnnnibpcajpcgglefindmkaj/http://www.dodccrp.org/events/9th ICCRTS/CD/papers/118.pdf
10. KRULAK. (1996). Command and Control. In The Nature of Command and Control. Washington D.C.: Department of navy headquarters US marin corps.
11. McNealy. (1999). Best practice to develop situational awareness in dynamics. small group military settings, 10-15. file:///C:/Users/CATC/Downloads/Best_practices_to_develop_situational_awareness_in_dynamic_small_group_military_settings.pdf
12. Ramezanali. (2011). Effective model based on the role of leadership structure and information system in the field of crisis management . chrome-extension://efaidnbmnnnibpcajpcgglefindmkaj/https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=93de7c779e1238c7eff1771f9421041c74167bff

13. Smeets. (2023). The challenges of military adaptation to the cyber domain: a case study of the Netherlands.
<https://www.tandfonline.com/doi/full/10.1080/09592318.2023.2233159#:~:text=Whilst%20NATO%20speaks%20increasingly%20publicly,case%20study%20of%20the%20Netherlands.>
14. Staheli. (2016). Cloudbreak: Answering the challenges of cyber command and control. *Lincon laboratory Journal* volume 22,, 61. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ll.mit.edu/sites/default/files/page/doc/2018-05/22_1_5_Mancuso.pdf
15. Thibodeau. (2020). Information overload. A war fighters challenge. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/<https://www.cfc.forces.gc.ca/259/290/22/305/Thibodeau.pdf>
16. Uhm. (2011). command and control. Joint doctrine , 80. [Joint+Doctrine+Publication+5+Command+and+Control+EN-1%20\(17\).pdf](#)
17. USJO. (2011). Joint Operations. Joint Publication 3-0. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/<https://www.moore.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/JP%203-0.pdf>
18. USNI. (2020). The Side Effect of Tech for Decentralized Command. <https://www.usni.org/magazines/proceedings/2020/february/side-effect-tech-decentralized-command>