András Mező[1]

Command and Control of Multi-domain Operations

DOI 10.17047/Hadtud.2021.31.E.12

The command and control system of NATO's joint operations requires large scale command posts, large numbers of stuff, and spacious, big sized infrastructure that even to operate are cumbersome, but also are an extremely attractive target for the adversary due to its extensive infrastructure and large supporting staff. The Alliance will face unpredictable challenges in the future, extending beyond traditional operational domains such as space and cyberspace. On top of that, the operations will extent to the full spectrum of operations, that is from low-intensity peacetime military engagement to high-intensity war conflict. These trends will further increase the size of the command posts. This paper presents the requirements for future operational staffs and command posts, while trying to find answers to emerging challenges.
KEYWORDS: command and control, Multi-domain Operations, NATO, command posts

Multidomén műveletek vezetése és irányítása

A NATO összhaderőnemi műveleteinek vezetése olyan nagyméretű és nagylétszámú törzseket és kiterjedt, nagyméretű vezetési pontokat igényel, melyek működtetése nehézkes, de a kiterjedt infrastruktúra és a nagylétszámú kiszolgáló állomány miatt még ráadásul rendkívül vonzó célpontot is jelent az ellenfél számára. A szövetség a jövőben kiszámíthatatlan kihívásokkal fog szembenézni, melyek a hagyományos műveleti doméneken túl az űrre és a kibertérre is ki fognak terjedni, ráadásul a műveletek teljes spektrumában, azaz az alacsony intenzitású békeidőszaki katonai szerepvállalástól nagyintenzitású háborús konfliktusig egyaránt. Ezek a tendenciák tovább fogják erősíteni azokat a tendenciákat, melyek a vezetési pontok méretét növelik. Ez a tanulmány a jövő hadműveleti törzseivel és vezetési pontjaival szemben jelentkező követelményeket mutatja be, miközben igyekszik választ is találni a felmerülő kihívásokra.
KULCSSZAVAK: vezetés és irányítás, multidomén művelet, NATO, vezetési pontok

The future

Urbanisation. Since an increasing proportion of the earth's population lives in big cities, a growing percentage of armed conflicts must be fought in densely populated urban environments. The Alliance has no experience of fighting in heavily populated areas and the Member States have always tried to avoid urban fighting in the individual operations as well.[2] At the same time, however, the political, economic, cultural and transport significance of cities requires that the Alliance be able to fight in cities. The metropolitan environment, especially the mega cities of developing countries, presents many challenges and threats to

[1] NATO Allied Command Transformation, Norfolk. NATO *Transzformációs Parancsnokság, Norfolk*. e-mail: Mezo.Andras@hm.gov.hu. https://orcid.org/: 0000-0002-2932-7563
[2] Grau 1997, 46.

Allied Forces. In this environment, due to climate change, there is an increasing competition for scarce resources, the daily failures of congested urban public services and infrastructures keep the population on the brink of riot. The cultural, religious and linguistic frictions of the diverse populations of the densely populated cities cause constant tension, which, from time to time, manifests itself in riots. The weak and dysfunctional municipalities engage in hopeless bureaucratic fight against corruption, while the military-, militia-, police- and volunteer police forces (often using illegal means) fight against organized (international) crime. The handling of demonstrations and riots requires increasingly skilled special police forces, while increasingly effective and radical legislation is being introduced almost bounding the rule of law. Effective police and legal measures further radicalize the populace. In the huge chaotic system created by big cities terrorists, cyber criminals, and separatist organizations can easily hide or disguise their activities, as a result, law enforcement and military tasks must increasingly overlap. The human and social media networks deliver, transmit, and comment uncontrolled news at unprecedented speed and rate. Information is easy to manipulate, so the above-mentioned uncontrolled groups have option at their disposal influencing the feelings of the population and organizing unexpected and violent demonstrations. Hence, cities provide a favourable environment in every aspect for hybrid and asymmetric threats, disruptive centrifugal forces and elements, which pave the way for a peer or near peer army to confront NATO. NATO's stabilization operations or operations to regain urban environment will not be easy at all. The urban environment severely constrains Allied forces from manoeuvring to influence populations, retain or regain territory, and thus urban operations carry strategic risks and consequences.[3]

Technological dependency. Multinational companies are increasingly taking over the initiative to develop key military technologies. The overshadowing of state ownership will have three consequences for NATO:

1. The acquired technological knowledge puts a company or a group of companies in a monopoly position, thus making defence investments completely vulnerable. For example, financially strong firms currently dealing with artificial intelligence will soon dominate in this area. The trend of their development, the price and the distribution of their products will not be under state control, and the armies that purchase their products will practically privatize national security, thus they will have to rely on the company's products and updates.

2. On the other hand, company policy will always seek to maximize profits, which means that there will be no guarantee that the same sophisticated military equipment or software will not fall, directly or indirectly, in the opponent's hands.

3. The third consequence is perhaps the most serious. The ever-strengthening international companies and corporations already have a much greater global influence than a medium-sized and medium developed country. It is a matter of time when multinational companies realize the potential of their political influence over their financial capabilities and come up with an open claim for their interests.

[3] Clemente et al. 2019, 14.

NATO is faced with the dilemma of either accepting commercially available technologies developed by private companies, risking dependence on them, or developing its own military technology, assuming it will never be as high-quality and efficient as those developed by large companies.[4]

The changing nature of warfare. The nature of future conflicts will be radically different from the wars of past ages. Perhaps the word "war" itself will soon become obsolete. In the past, a war meant basically military operations, which started only after political, strategic decisions, during which large-scale land troops, air and sea fleets clashed. These battles and campaigns typically took place in a single domain and resulted in huge human and technological losses,[5] their purpose and result were to come into possession or control and retain sea routes. The command and control of the combat units were carried out through a strictly regulated chain of command. In the future, however, military forces will be no longer sufficient to resolve future conflicts, but all instruments of national power will have to be used: diplomatic, information, economic, and psychological tools as well. Military assets alone will only be able to achieve very limited objectives. The components of national power should be applied internally by Alliance member states to build their own resilience, such as cyber defence and control over the financial and energy sectors. And, of course, it must be applied externally to influence the global situation, for example, in the communication with international institutions. The increasing importance of other factors of national power (diplomatic, information, economic), the expansion of the operational environment (political, social, infrastructural, etc.) and, within that, the expansion of the military operational environment to new domains (space and cyberspace), will result in the escalation of conflicts without any formal, state-level, strategical decisions, for instance in cyber domain.[6] Attacks launched in cyber domain can be well disguised, easy to deny, but can have strategic, political consequences and create the basis for further attacks or attacks in other domains. Therefore, the Alliance and the member states must have adequate cyber defence, which is active not only in state of war but practically always. Because the cyber war is already upon us.

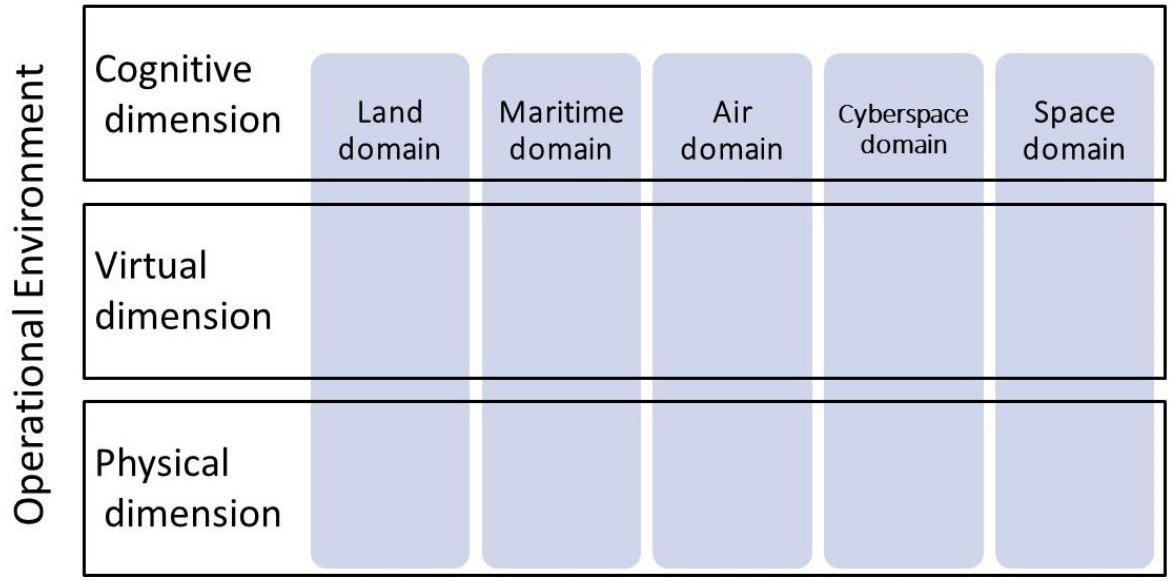
Prior to future conflicts, pre-deployment of combat units must begin before strategic and political decisions are made. However, future combat forces are no longer just conventional joint or all-branch land units, but multi domain task forces and battle groups capable of performing synergistic, unified, simultaneous, integrated, and mutually supportive (cross-domain) operations across all five domains, through the depths of enemy. High-precision and / or special operations strikes are aimed at reducing the adversary's military-economic potential, destroying critical military and civilian infrastructures that are essential but without collateral damage or civilian casualties. They also use new disruptive revolutionary technologies such as robots, artificial intelligence, and weapons based on new physical

[4] Zsebe 2020, 1.
[5] On Land, in air and on sea. In rare cases, cross-domain maeuvre had also occurred. Interestingly, in 1795 in the Zuiderzee Bay, the Dutch fleet, stationed at Den Helder harbor and frozen at anchor, was occupied by French light cavalry. However, after the First World War, co-operation between domains became ever closer and more frequent.
[6] Rejcek 2019, 1.

principles. Contrary to traditional chain of command, multi domain operations are managed in a single information space.

In the (near) future, warfare will extend to new domains and new dimensions. The new domains (space, cyber) are unlikely to appear at tactical level, but at operational level there are significant opportunities for using the cyber domain and the virtual dimension. At tactical level, the physical environment (such as air, land, sea) has a much greater impact on activities, and the potential of cyberspace is not direct enough to be considered at this level.[7]

Command and control. What will this mean for the future command and control? The Command and Control (C2), which was traditionally created to coordinate kinetic activities in one of the domains in order to achieve physical effects, will coordinate in its new role the new non-kinetic and kinetic activities across all of the five domains, with effects primarily in the cognitive, virtual dimension. This means that the Operational Level Command Post (CP) will employ non-kinetic operations, cyber and social technologies and tools.



1. Figure

Domains and dimensions in the Operational Environment

(Source: Ducheine, P.: NATO' s challenges in Multi-Domain aka Full Spectrum Operations, presentation)

The characteristics of leadership will change shortly. The decision-making process and, at lower echelons, the troop leading procedures will be rewritten by the usage of artificial intelligence in the CPs to support decisions. Mission-command leadership continues to evolve until the point where subordinate staffs, CPs, and commanders will be able to continue their mission seamlessly, even if they lose contact with their superior command. For the sake of better mission command a mobile, fragmented, networked system of CPs must be developed. The individual CPs in this network can take over the role of each other even in the event of barrage jamming or detriment of a significant part of the system, thereby significantly reducing the vulnerability of C2 to both cyber and kinetic attacks. Last but not

[7] Clemente et al 2019, 15-18.

least, the operational CPs must be capable of cyberspace operations and operations in social media in order to be able to exert decisive influence in the cognitive and virtual dimensions.

Changes in the organizational structure of the CP are also required to accommodate other functions. However, coordinating all components of national power is definitely not a military task, operational level staff must gather and process information in a way that can be interpreted by other (strategical level) actors in the whole of government approach and thus military planning is fully synchronized with diplomatic, economic, etc. efforts. The interaction between military and non-military entities requires new structures and new decision-making processes to allow for decisions to be made in a timely and synchronized manner. The technology is changing the way information is processed and disseminated, and requires further changes in decision-making, in the way military organizations are managed and structured.[8]

Operational Command Post

Today's military organizations have been established at strategic, operational and tactical levels. This organizational structure is suitable for conducting extensive operations, ensuring a link between strategic objectives and tactical activities. The basic function of the command post is to support the commander's decision-making and to provide the necessary infrastructure for the transmission of decisions to subordinates. The ever-growing area of operations, the complexity of the battle, and the increasing amount of information, require more and more experts, analysts, and bigger and bigger staff. The operational staffs try to give the commander an accurate picture of the situation and outline possible scenarios, but the working speed of the staffs is often just behind the pace of the operation, thus by the end of the 20th century, mission command[9] leadership had become commonplace. The NATO-wide accepted mission command enables the staff to make autonomous decisions within their delegated authority and limits, and to take advantage of their better situation awareness. The delegation of tasks and decision-making authority restrained the growth of the staff to a certain extent, but they are still huge, inflexible organizations that are burdened with internal communication problems and due to their relatively large size, they can be easily identified and attacked. For a peer enemy, the Alliance's command and control system is not only an attractive target, but also an opportunity to use high-precision and destructive weapons therefore the future command post will be a system of mobile, fragmented, hidden cells of the CP.

Disruptive technology in Command Posts

Operational CP in the technological sense is a huge information node, where inputs are the intelligence, reports, commands and after processing of those the outputs are the commands, directives, instructions, guidance. In the future, as information technology advances, the

[8] Clemente et al. 2019, 19–22.
[9] Mission Command has no NATO agreed terminology, yet.

amount and the quality of incoming input will continue to improve and the transmission and processing speeds increase as well. The widespread usage of networking IT tools reduces information security and efforts should be made to find a reasonable balance between the need for information sharing and the effectiveness of C2.

Artificial Intelligence (AI) will facilitate the analysis and extraction, the interpretation, and analysis of huge amounts of data, and will support decision-making through pattern recognition, and some prediction. AI will have no problem tracking the evolution of higher-level strategic political, military, economic, social, information, and infrastructure (PMESII) factors and the narrower, operational-level diplomatic, information, military, and economic (DIME) situation, while still has remaining capacity for processing tactical level sensors' data.

The inexpensive and secure storage and extensive sharing of vast amounts of data enables the creation and maintenance of a Common Operational Picture (COP) of the various CPs. The storing, processing and analysing of images, videos records captured by sensors of various platforms or by cameras, will allow to analyse patterns of movement of the local population, to identify unusual changes, or new faces, strangers, compare their biometric data with other databases, thus identify dangerous elements, criminals and trends.

2. Figure
The commander uses virtual reality to study the situation
(Source: Virtual Reality Command Centers)

AI makes it possible to reduce the size of CP, while developing different courses of action and scenarios much faster and quantifying their advantages and disadvantages. Moreover, AI is able to present the commander not just the current tactical and operational situation by using its simulation and virtual capabilities, but also able to demonstrate the Commander's intent to his/her subordinate, the courses of actions, and their first and second order effect. AI uses Virtual Reality (VR) and Augmented Reality (AR) for visualizing the situation and courses of actions. While VR is a synthetic representation of the real world, in AR it is possible to project synthetic elements into reality.[10] For example, the commander

[10] Ventura et al. 2018, 1.

understands the situation report (input) by using VR and will express his intention (output) by using AR projected onto subordinates' helmet screen.

2. Figure

Subordinates understand the commander's intentions through augmented reality

(Source: Military Aerospace Electronics)

Initially, AI tools will not be perfect at all, and for a long time, they will only complement and support the command decision-making, but in the future the trust will build-up of and operational level staff will increasingly rely on AI suggestions and there will come the time when the AI system will get a degree of autonomy.

Levels of AI autonomy[11]:

0. level: Manual control – with no assistance from a system;

1. level: Decision support – by the operator, with input in the form of recommendation provided by a system;

2. level: Consensual AI – by the system, with the consent of the operator required to carry out actions;

3. level: Monitored AI – by the system to be automatically implemented unless vetoed by the operator; and

4. level: Full automation with no operator interaction.

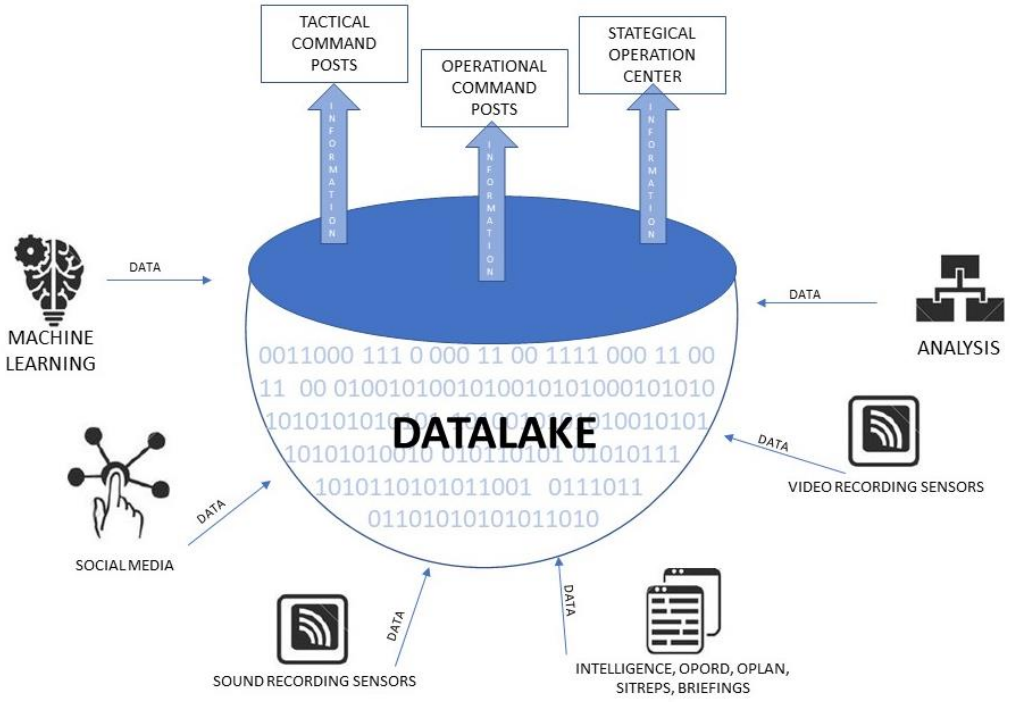
The latter may seem a fearsome possibility and raise obvious legal and ethical questions if AI is to decide to kill human, but it will be an inevitable necessity, for example, in cyberspace and space operations. In these domains, events occur at a rate (minutes, seconds) inconsistent with human detection and perception, to which humans would be unable to develop an adequate (timely and appropriate) response.

While the full spectrum of AI technologies can be useful at operational level, research must be narrowed and focused on areas of critical importance, such as uncertainty, unstructured data, use of probing interventions to identify enemy intent, use of small samples, dirty data, high clutter environments, highly heterogeneous data, adversarial AI, and machine

[11] According Clemente, Streefrkerk and Scherrenburg manual control is level 1, but they fail to explain why, therefore I renamed this level to level 0.

learning in contested and deceptive environments, to name just a few, explain ability and meaningful human control.[12]

The form in which data and information are stored in a data cloud is extremely important for further analysis. The data cloud should rather a Data Lake instead of a traditional data storage centre, which is a repository of large amounts of data in native raw format. This lake will facilitate further analysis, queries and will eventually result in a much more complete understanding of the situation. Data Lake will provide the ability to collect and store large amounts of raw data at a low cost, be able to store many types of data on the same site, be able to transform data, define its structure at the time of usage, and perform data processing.[13]



1. Figure

The Data Lake concept

(Source: author based on Clemente, Streefkerk, Scherrenburg[14])

Analysis of joint functions

AI is (or can be) a huge step forward in C2 of multi-domain operations

The joint functions are a framework that provides the commander and staff with a means to visualize the activities of the force and to ensure all aspects of the operation are addressed. They are a point of reference, as well as a description of the capabilities of the force. The commander needs to consider the joint functions, both when determining the capabilities required for a joint force and when conducting the operation. The joint functions are:

- manoeuvre;

[12] Clemente et al. 2019, 31.
[13] Groleik 2020, 1.
[14] Clemente et al. 2019, 32.

- fires;
- command and control;
- intelligence;
- information activity;
- sustainment;
- force protection; and
- civil-military cooperation (CIMIC).[15]

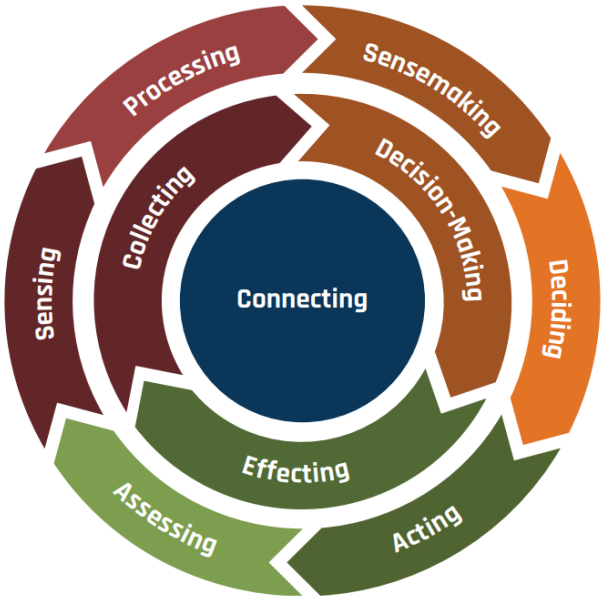
Manoeuvre. Situational Awareness (SA) is essential to the manoeuvres of the Allied Joint Commander. SA is not limited to knowing one's own and the opponent's forces, but extends to the physical environment (terrain, weather, geography and hydrography), as well as social environment and cyberspace. The SA should be shared with subordinate and other governmental and non-governmental actors. The right combination and quantity of different sensors provides reliable and mutually supportive data. The sensors not only upload the detected object's location, location, and targeting data to the data lake, but they also communicate with each other. They also share and direct each other to obtain additional data or to clarify or refine existing data. By interpreting the raw data available in the data lake, AI converts it into intelligence and then provides comprehensive SA. SA facilitates the conduct of an Operations Assessment and comparison of the actual situation with the original Operational Plans.[16]

AI helps the staff to better develop and analyse Measures of Performance[17] and Measures of Effectiveness[18] and identify trends. AI will be able to predict the potential consequences of course of action, explore their potentials, benefits and risks, will offer alternatives and variants of them. It develops concept of operation and suggests manoeuvres of available combat force. Propositions from AI will be strange to conventional military thinking in the beginning because it will offer unexpected solutions that would not have come up in traditional military staff work. AI evaluates whether the specified operations and operational effects are suitable for achieving the operational objectives or need to be modified.

The greatest impact of disruptive technology on manoeuvre will be real-time situational awareness. Modelling and simulation offer many more opportunities for the operational staff to conduct wargame to find the best course of action to achieve operational objectives. As always, the model must reflect reality as accurately as possible, i.e. it must be directly related to the operational picture in the data lake. This link will update not only the situation of the friendly and the enemy forces during modelling and wargaming, but the intelligence on the population, governmental and non-governmental actors will be also refreshed.

[15] AJP-01 (E) 2017, 4-2.
[16] Clemente 2019, 38.
[17] Measures of Performance (MoP): Not NATO agreed terminology. Definition: A criterion to assess friendly actions that is tied to measuring task accomplishment. (source: NATOTerm)
[18] Measures of Effectiveness (MoE): NATO agreed terminology: A criterion used to assess changes in system behaviour, capability, or operating environment, tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (source: NATOTerm)

Fires. This joint function allows achieving operational objectives by synchronizing kinetic and non-kinetic activities against your opponent. Joint targeting[19] helps to determine the effects needed to achieve the commander's goals, and the activities needed to create those effects, helps to select and prioritize targets, coordinates the capabilities available, and assesses the cumulative effectiveness of capabilities. AI can make suggestions for choosing targets, defining the fire assets and the tools needed to implement, but for ethical reasons, of course, the final decision must always be made by a human operator.



5. Figure
C2 cycle
(Source: C2 Capstone Concept)

Command and control. In 2018, NATO introduced a new command and control concept.[20] This command and control theory has replaced the OODA loop[21] that has been used for a long time, but similarly, the purpose of the cycle is to prevent the opponent's decision cycle from running faster, thus gaining a leadership advantage. The inner ring shows the C2 phases and the outer ring represents the functions and activities. In the future, this C2 cycle will no longer work with the extensive involvement of human resources, but relying on AI and other disruptive technologies will speed up each step of the cycle individually, thus intensifying the entire cycle.

At the heart of the new concept of C2 is connecting, which links and harmonizes the three main stages of the model. The connection involves the aggregation of manual, semi-automatic and automated communication and information capabilities needed to connect the actors and the various platforms.

[19] Targeting: NATO agreed terminology: The process of selecting and prioritizing targets and matching the appropriate response to them, taking into account operational requirements and capabilities. (source: NATOTerm)
[20] Command and Control (C2) Capstone Concept, 2018.
[21] The term itself originates from US Army Colonel John Boyd. The abbreviation stands for Observe, Orient, Decide, Act.

The infrastructure and the time needed to build, set up, and relocate Command Posts (CP) represent a critical vulnerability. The CP that have not yet been built cannot lead really, so the commander is forced to relocate the command post incrementally in order to maintain the continuity of leadership. The infrastructure needed for the CP needs to be split, the old one maintained, the new one sent forward and then the staff is to move in several stages when the new CP is complete. The commander is also forced to split the forces providing security and force protection. In addition, the concentration of antennas and facilities, increased vehicle traffic due to relocation to a specific location clearly signals the existence of a CP and becomes a high value target for the enemy.

Today's state-of-the-art reconnaissance and artillery systems represent a serious threat to an operational-level CP. The key to future CP protection is to hide, disguise, and relocate frequently. Despite such measures, the destruction or neutralization of a CP is still possible, and secondary backup management structures are needed to ensure the continuity of command and control capability at operational level. Therefore, the solution to prevent the neutralization or destruction of operational CPs is their scattered and fragmented deployment. The CP of the future is a series of tiny, decentralized cells in constant motion, always connected to each other, but with as little physical and electromagnetic radiation as possible. With the help of new communication technology, CP cells would not concentrate on a specific area, would not represent valuable target to the enemy and would blend into the environment, since hardly detectable.

Of course, providing a flow of information to a decentralized staff requires an approach completely different from today's information and knowledge management. Today, staff officers communicate with each other through word processing programs, outlook and less frequently through power point presentations. It imposes a huge workload on the staff trying to present reality by slides and texts. With augmented reality, scattered staff elements will be able to visualize information without having to draw it on paper or otherwise distort it.

Future CPs will receive and send huge amounts of inputs and outputs over a network of multiple nodes and communication paths to connect the staff or CP elements wherever they are. Jamming or destroying the elements of the network does not prevent information flow, as AI, like today's Internet, will also be able to connect through the elements of the remaining network. Staff elements will be able to continue discussions, briefings, and meetings in virtual reality without being physically in one place. This would reduce the size of the CP, increase decentralization and the ability of a dispersed deployment, and improve the rhythm of decision making by making them more efficient and flexible.[22]

Intelligence.[23] Intelligence in the traditional sense provides the commander with the knowledge about the area of operation (terrain, weather), enemy location, strength, composition, capabilities, current and expected activity. However, recent conflicts have significantly changed this perception and it has become evident that intelligence can only be

[22] Clemente et al. 2019, 37–39.

[23] Intelligence: NATO Agreed terminology. The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers. (source: NATOTerm)

effective if the CP is able to provide the commander with relevant knowledge about all the systems (political, military, economic, social, infrastructure and information) in the Area of Operation and about their effects and interactions.

The operating environment is defined as: "a composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander."[24] It is inclusive of all actors and actions. It encompasses the physical and non-physical areas and factors relating to maritime, land, air and space, information and cyberspace. In NATO, therefore, the operating environment is usually described by a number of interconnected elements including political, military, economic, social, information and infrastructure (PMESII). PMESII analysis enables commanders and staffs to understand the operating environment from which the Alliance is able to create effects by using the instruments of national power (in a synchronized way).[25]

The starting point for joint intelligence is the available raw data from which information can be generated. The raw data can come from a variety of sources, such as sensors, information provided by strategical command, subordinate situation reports, or open sources. The format of the data can also be varied: written reports, photographs, videos, and audio recordings. It is an enormous challenge the unmanageable amount of data, its registration, storage, updating and processing. A solution may be that AI-controlled sensor complexes can adjust themselves their sensor settings to transmit only records of substantial quality that have been pre-filtered or interpreted at some level. The incoming records processed by AI allows to reduce the number of staff officers (analysts) and provide balanced, objective intelligence. Both strategical and tactical commands are able to retrieve the Joint Common Operational Picture (JCOP) developed from data lake. [26]

Information. New communication technologies, especially social media technologies, are not only empowering governments, institutions and media to shape public opinion, but also enable the operational CP to inform the local population in a meaningful way, to convey the narrative of NATO and to influence it in order to achieve operational objectives. However, social media can be not only an appropriate means of conveying NATO messages, but can also be used to raise situational awareness of the CP and to improve the exchange of information between partners, particularly NGOs.

At operational level, information activities are supported by Level 1 AI (Decision Support) in contributing to the analysis, and to the evaluation of the information environment and to the targeting process. AI and machine learning help you identify your target audiences and design PSYOPS and media campaigns more effectively. Similarly, AI helps identify bots (such as social media bots) that try to publish misleading or irrational information, or to arouse anti-NATO emotions by spreading fake news.

Deciding whether or not NATO is authorized to use bot-based social media tools to create opinion trends is entirely theoretical. For a long time, our opponents have been

[24] Political guidance on ways to improve NATO's involvement in Stabilization and Reconstruction, 2011, paragraph 17.
[25] AJP-01 (E) 2017, 1-5.
[26] Creating a Joint Common Operational Picture is part of the Federated Mission Network project.

successfully using information operations to loosen NATO and EU political cohesion, so giving them cyber domain would be like give up the air or space domain. Of course, the Alliance's credibility requires that the social media toolkit be used by NATO, after making decisions at the appropriate political level, within an ethical and legal framework. On the other hand, however, these principles and values are by no means universal and are not respected by all nations. It may come up as a solution for example, the privatization of these cyber services, that is, outsourcing to private providers, could be involved, which would significantly simplify the resolution of legal concerns and could easily be denied. Our adversaries, for instance, did not hesitate to "outsource" their military cyber operations or rely on "patriots" in their foreign information operations. These issues need to be resolved very quickly, since in cyberspace “the first shots have already been fired”. [27]

Sustainment. Forces and their fighting power need to be sustained through all phases of operations. Sustainment provides for the comprehensive provision of: personnel; logistics; medical; and general MILENG support required to maintain combat power throughout all phases of the operation.[28] The sustainment system will take advantage of disruptive technologies to meet the requirements of multi-domain operations. Real-time status reports (data input) uploaded into the database by an increased number of sensors allow logistics delivery systems to meet realistic logistics needs instead of relying on past experience and usual standard norms. The calculation of actual logistical needs will begin with data from real-time sensors, which will be processed by AI-based predictive models. The system delivers not only the supplies that meet the current needs of the subordinate units, it also takes into account the possible changes of the operational situation and sends the modified supplies directly to the combat units. The autonomous transportation systems (UAVs, self-propelled vehicles) allow you to diminish the level of logistics stages and deliver supplies directly from the strategic level depots to the combat level user without wasting time on forward staging and endangering human life with complicated convoy operations.

This improves coordination between operational and logistics planners and will reduce the labour-intensive, expensive system that requires large warehouses and records, which overloads the logistic stages. The logistics planner provides a better overview of the logistics situation, and can more quickly assess and predict the logistical impact of the operational action options because it has an overview of the ongoing operation (situational awareness). Modelling and simulation (AI) can also simulate the logistical impact of an operation.

AI will offer Allied Joint Force Commanders the ability to optimize logistics networks to sustain combat capability. AI can help the staff change the nature of the logistics operations. Proactive planning instead of reactive, accurate forecasting instead of assumptions, autonomous control instead of manual control, personalized service instead of standard services, this is the future of maintaining combat ability (sustainment).

The extensive usage of bio sensors also improves operational-level medical logistics and its automation. Sensors that monitor the health of each soldier automatically transmit measured data to the data lake, AI continuously monitors, links it to past health records, and

[27] Clemente et al. 2019, 48-49.
[28] AJP-3(C) 2019, 1–24.

makes (or takes) actions when necessary. During the evacuation process, the status of the casualties is continuously monitored by its sensors, and, depending on their condition, AI continuously adjusts their triage level, proposes (or arranges) the optimal distribution and reception of patients in medical facilities, and prepares life-saving interventions. However, this is only a tactical level. At operational level, AI draws attention to mass illnesses and losses and, depending on the level of AI, proposes or reallocates targeted health instrument and resources.[29]

Force protection.[30] At operational level, coordination and integration of all the elements of force protection (FP) are essential to ensure overall force coherence effectively. The composition of the various FP elements is determined by the threat level, the scale of the operation, the climate and the civil environment. In a low-intensity conflict, security and health protection may be the only essential element needed. As the threat level increases, additional precautionary (force protection) measures may be required, such as air defence, explosive ordnance disposal (EOD) and chemical, biological, radiological and nuclear (CBRN) protection. However, hybrid threats may exist at any level of intensity, and therefore, require the application of protection measures, tasks, and activities across the entire spectrum.[31]

To the freedom of action of NATO operations the security[32] is essential, as well as restraining enemy activities and reducing the vulnerability of own forces. The concept of NATO security includes access and control, physical security[33], operational security, counter-intelligence[34], information operations and activities, computer, cyber, personal and air transport security. Disruptive technologies such as AI facilitate these activities, especially information activities and cybersecurity. The cyberspace domain is particularly well suited for the employment of AI: controlled or fully automated (level 3-4) AI is capable of detecting cyber-attacks and responding and recovering damages immediately. An operational CP is not capable of analysing all threats within a reasonable timeframe and developing adequate responses. There are tremendous opportunities for AI and machine learning in the implementation of FP. The use of disruptive technology solves the problems encountered in FP: the human factor, labour intensive tests and analyses, human bias, lack of experience, lack of professionals, experts, etc.

[29] Clemente et al. 2019, 50–52.
[30] Force protection: NATO agreed terminology. All measures and means to minimize the vulnerability of personnel, facilities, equipment and operations to any threat and in all situations, to preserve freedom of action and the operational effectiveness of the force.
[31] AJP-3.14 (A) 2015, 3-2., A-1
[32] Security: NATO agreed terminology. The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion, terrorism and damage, as well as against loss or unauthorized disclosure. (source: NATOTerm)
[33] physical security: NATO agreed terminology. That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, documents and information, and to protect them against espionage, sabotage, terrorism, damage, and theft. (source: NATOTerm)
[34] Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism.

Civil-military Cooperation (CIMIC)[35]: Although the greatest difficulty in exchanging information between the civilian population and the operational command posts is not technological in nature, there is still room for improvement. One of the manageable difficulties is the inadequate exchange of information between NATO and international NGOs, mainly due to the lack of interoperability. The Federated Mission Networking (FMN) project aims, among other things, to improve civil-military interoperability. Another challenge that can also be addressed is when, on the contrary, there is too much data available and there are not enough staff officers to process it and therefore the decision-making is paralyzed. AI, just like intelligence, can provide a solution that can facilitate information management in civil-military cooperation.

Summary

The joint functions provide a framework for managing a huge amount of information (sensing, processing and executing), displaying, depicting, and taking into account all aspects of an operation, and clearly defining the commander's intent. As you can see, AI is (or can be) a huge step forward in C2 of multi-domain operations.

Suggestions, conclusions:

The most important capability of the CP of the future is that the staff functions are distributed among several small cells of command points, so that the commander remains able to oversee the situation and communicate his/her intentions clearly to his/her subordinates. Nevertheless, the small cells, the J structure, should be able to stay in touch with each other, share their information and take over each other's tasks, replace each other in the event of disruption or destruction of the other.

Access to unclassified and classified networks and the automatic exchange of encrypted information are essential. The widespread use of virtual and augmented reality must be ensured in order to maintain a continuous connection between the commander and his/her physically distant staff. It is vital for the operation commander that information is exchanged securely and controlled, not only with the subordinate headquarters but also with the strategic level, the whole of the government actors, the international and non-governmental actors as well.

The future commander must be able to act in the cyberspace domain and gain superiority in both the cognitive and virtual dimensions.

For successful manoeuvres, the joint commander must have situational awareness that can be easily shared with subordinates, superiors, and with NGOs as well. Supervised (level 3) AI is capable of filtering data, establishing and combining relationships, and displaying the information thus generated in a JCOP. Data analysis techniques and supervised AI will allow the staff to understand the current situation and compare it to the end position required in the operational plan. AI helps the operational staff develop and analyse Measures of Performance

[35] Civil-military cooperation: NATO agreed terminology A joint function comprising a set of capabilities integral to supporting the achievement of mission objectives and enabling NATO commands to participate effectively in a broad spectrum of civil-military interaction with diverse non-military actors. (source: NATOTerm)

and Measures of Effectiveness and trends. Modelling and simulation offer the opportunity to run numerous war games to determine the best way to achieve the goals. The transmission of information between the JCOP and the simulation model is direct and automatic, so action scenarios are modelled in the virtual environment closest to reality.

In targeting, supervised AI selects and prioritizes targets, but in the short run, still an operator will be required to verify and approve (consensus AI). However, in the future, as soon as confidence in the system is established and the system is able to fully understand the commander's intent, automation will advance to Level 4. Virtual and Augmented Reality allows for reducing the size of CPs and scattered, decentralized deployment while enhancing the efficiency of information flow.

AI-backed intelligence enables the commander to gain a deep insight into the political, military, economic, social, infrastructure, and information dimensions of the operation. The availability of data and the processing of relevant information are essential. Creating the Data Lake provides a common operational picture for all command and control levels (tactical, operational and strategic). The collection, selection, and processing of huge amounts of data require high level of automation.

At operational level, information (as well as psychological operations and public relationships) will be supported by decision support AI (Level 2) by analyzing and evaluating the information environment and contributing to the (kinetic and non-kinetic) targeting process. AI helps to identify the target audiences and plan psychological and media campaigns more effectively. AI helps identify bots (such as social media bots) that try to send misleading or irrational information, bombing the target audience with false information, and provoke anti-NATO sentiments.

The use of disruptive technology to sustain combat capability enables logistics systems to play an increasingly active role and proactively.

AI will support security tasks during force protection, with particular emphasis on cybersecurity. The advantage of AI is based on a (near) real-time analysis of risks and threats, resulting in the rapid development of coordinated counter actions.

In conclusion, artificial intelligence is a crucial prerequisite for managing multi-domain operations. The unanswered question is how, in the absence of disruptive technology, command and control can remain effective in future operations across five domains.

SOURCES

AJP-01 (E) ALLIED JOINT DOCTRINE, Edition E Version 1, NATO, 2017. February.

AJP-3(C): ALLIED JOINT DOCTRINE FOR THE CONDUCT OF OPERATIONS, Edition C Version 1, 2019. February.

AJP-3.14 (A): Allied Joint Doctrine for Force Protection, Edition A, 2015. NSO.

Groleik, Alex 2020. Introduction to Data Lakes, https://www.oreilly.com/library/view/the-enterprise-big/9781491931547/ch01.html, (Retrieved: 07th March 2020.)

Command and Control (C2) Capstone Concept Version 0.5 (draft), Norfolk: Allied Command Transformation, 25 July 2018.

Clemente et al 2019. Frederico Clemente, Jan Willem Streefrkerk, Marcel Scherrenburg: *The Future of the Command Post*, Utrecht: NATO Command and Control Centre of Excelence, 2019.

Grau, Lester W. 1997. Bashing the laser range finder with a rock, *Military Review* 78. (1997. May-June): 46-55. o.

Rejcek, Peter 2019. Undeclerad wars in Cyberspace are becoming more agressive and automated, https://singularityhub.com/2019/08/01/undeclared-wars-in-cyberspace-are-becoming-more-aggressive-and-automated/, (Retrieved: 15. March 2020.)

Political guidance on ways to improve NATO's involvement in Stabilization and Reconstruction, 2011, paragraph 17. https://www.nato.int/cps/en/natohq/official_texts_78314.htm, (Retrieved: 15. March 2020.)

Ventura et al 2018. Sara Ventura, Rosa M. Banos, Cristina Botella: Virtual and augmented reality, https://www.intechopen.com/books/state-of-the-art-virtual-reality-and-augmented-reality-knowhow/virtual-and-augmented-reality-new-frontiers-for-clinical-psychology, (Retrieved: 7th March 2020.) DOI: 10.5772/intechopen.74344

Zsolt, Zsebe: A katonai magánvállalatok szabályozása a nemzetközi jogban, https://biztonsagpolitika.hu/elemzesek/a-katonai-maganvallalatok-szabalyozasa-a-nemzetkozi-jogban, (Retrieved: 05 March 2020.)