



# Evolution from the Network-Centric Warfare Concept to the Data-Centric Operation Theory

A. Skoryk\*, B. Niziienko, A. Dudush, V. Shulezhko and I. Romanchenko

*Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine*

The manuscript was received on 24 June 2020 and was accepted after revision for publication as technical information on 22 June 2021.

## Abstract:

*The article analyzes the impact of disruptive technologies on the evolutionary development of military architectural frameworks and concepts of warfare. It argues the need for a transition from the Network-Centric Warfare concept to the Data-Centric Operation theory and proposes a 4D-extensional representation of the combat space of weapon systems integrated into a single network. It is concluded that there is hardware redundancy in modern weapon systems and it is possible to use it as a network resource, the management of which provides additional opportunities for improving operational capabilities.*

## Keywords:

*data-centric operation, network-centric warfare, 4D architecture, system of systems*

## 1 Introduction

“The very first, most principal and most important decision in terms of consequences that a statesman and commander must take is to determine the type of war he is plunging into ...” (Karl von Clausewitz, On War) [1].

It is clear that the technological advantage on the battlefield is not enough to win. There are many examples in history when, with the help of outdated weapons, a victory was achieved over an adversary with technical superiority. However, there are much fewer examples of victory over the enemy that used more advanced methods and innovative concepts of warfare, and those are usually associated with “covering the enemy with the corpses of your own soldiers”.

There is the concept of Disruptive Technology – an innovation that can completely supersede an existing technology, product or service [2]. In military affairs, the advent of destructive technologies leads to a change in the concept of warfare.

---

\* Corresponding author: Antiaircraft Missile Troops Department, Kharkiv National Air Force University, Sums'ka st. 77/79, Kharkiv, UA-61023, Ukraine. Phone: +380 50 302 35 09, E-mail: anatolii.skoryk.65@gmail.com

At the end of the twentieth century, the development of arms of the NATO countries came to a certain point of bifurcation. Despite the most modern weapons, the navy, aviation, and ground forces on the battlefield began to experience significant difficulties in conducting joint operations. The development and complication of armaments required new concepts for their joint use on the battlefield, which would be based on advanced achievements of control and communication technologies. And such a concept was formulated – Network-Centric Warfare (NCW) [3-5].

In this case, it is necessary to distinguish between the concept of NCW – as some fairly abstract concept [3], C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) – as the architecture for building promising combat systems [6], and the C4ISR architecture framework (AF) – a specially developed set of tools for designing various architectures of combat systems [7].

It should also be noted that over the 25 years that have passed since the inception of the NCW concept, a number of cardinal technological changes have accumulated. Military AF have come a long evolutionary path in their development. Network space has become familiar to humans. This is fairly easy to verify by simply pulling out your smartphone and realizing that the network problem no longer exists. Networks are available to you literally at your fingertips. We again approached the next point of bifurcation - the choice of a further development path. And here it is appropriate to quote from the work “All that glisters: Is network-centric warfare really scientific?": “We share with the NCW proponents the view that the emergence of information and communications technology presents great opportunities to the military profession. ... Nonetheless, we contend that the nature of the potential and the best way to implement change are very much open to debate, and we submit that there are serious questions regarding the status of the NCW thesis as a secure and reliable basis for making capability development decisions” [8].

In our opinion, one of the possible ways of further development is the creation and use of the new Data-Centric Operation theory (DCOT).

Data-Centric Operation theory is a new vision of combat systems; it is a transfer of 4D extensionalism to the operational level, it is metamorphisms, cloud-computing and service-oriented architecture not only in virtual networks, but also on the battlefield. Data-Centric systems are “werewolf” systems that do not have a constant “body” (structure), constantly changing “metamorphs”, whose heart (command posts) are difficult to detect and are inaccessible to the enemy; some of them can be in virtual structures – clouds. Such combat systems are difficult to destroy with conventional (lethal) weapons.

The purpose of this article is to analyze the influence of destructive technologies on the evolution of the Network-Centric Warfare concept and military AF, as well as to justify the inevitability of the transition from the NCW concept to the DCOT.

## 2 NCW Concept and C4ISR Architectural Framework

There is a correspondence between the level of complexity of the control system and the level of complexity of *the control object*. The more complex *the control object* is, the more complex the control system must be. If the control system is unjustifiably complicated in comparison with a relatively *simple object*, this entails unnecessary costs, duplication of functions, additional communications, reduced efficiency, etc. On the other hand, an attempt to control *a complex object* using a primitive (in its

structures, functions, methods, information technologies) control system will also inevitably lead to a decrease in the effectiveness of the combat use of weapons [9].

The problem of ensuring such compliance is systemic in nature. Therefore, its solution was sought in the field of developing a new class of System of Systems (SoS) – C4ISR. The onset of C4ISR is associated with an article by Admiral William Owens [6] published by the Institute for National Security Studies. In this paper, it is noted that the revolution in military affairs (RMA) is associated with the synergy of three main categories: intelligence, surveillance, and reconnaissance (ISR); C4I – command, control, communications, computer applications, and intelligence processing; and *precision force (PF)*.

Admiral Owens was well aware of the continuity of the control system (C4ISR) and the *control object (precision force)*. However, financing had to be directed to the most breakthrough areas, which is probably why the concept of C4ISR, rather than C4ISR\_PF, became popular.

The Joint Architectural Commission of the United States Department of Defense, developing C4ISR, considered the task of creating AF as evolutionary. Therefore, the first version of the Architecture Framework C4ISR, published on June 7, 1996 [10], was already replaced in December 1997 by C4ISR V2.0 [7]. In the new version of AF, an understanding of architectural descriptions as work products is already beginning to take shape, so the three architectures have been replaced by *an architecture view* and the fourth one – *all views*, has been introduced, which defines high-level guidelines for using AF to describe architecture and it contains general basic recommendations, descriptive models and data. The architecture has been developed in accordance with a specific area and in a specific context (Fig. 1). We will not dwell on all the features of C4ISR AF, as this question is sufficiently covered in many works on this subject, for example [7, 10, 11]. We will only briefly comment on the issue.

C4ISR AF is a “product-centric”. Various architecture description elements (graphic, textual, tabular) being developed during the construction of the architecture are combined by the term “architecture products”, among which there are essential products that declare common approaches (methodology) to the design of various weapons systems and supporting products of the C4ISR architecture – architectural solutions determined by the specialization of the developed weapon systems. Each one of the Framework products was considered a data entity. Fig. 2 presents the high-level data information metamodel C4ISR AF V2.0 [11], demonstrating the interconnections and relationships between data elements.

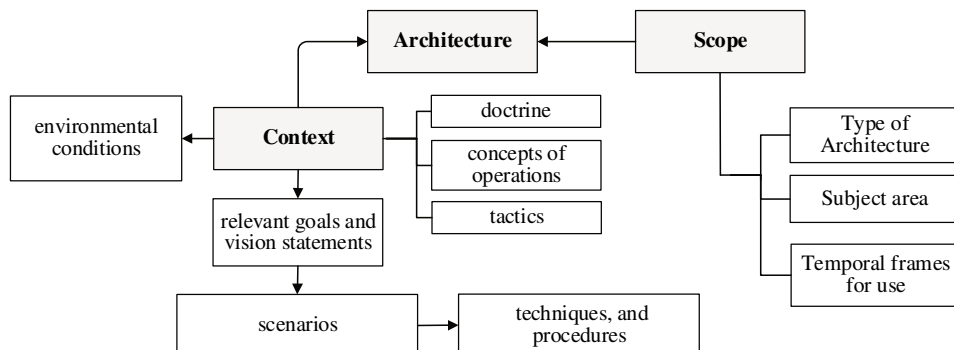


Fig. 1 Conceptual architecture design diagram in C4ISR AF

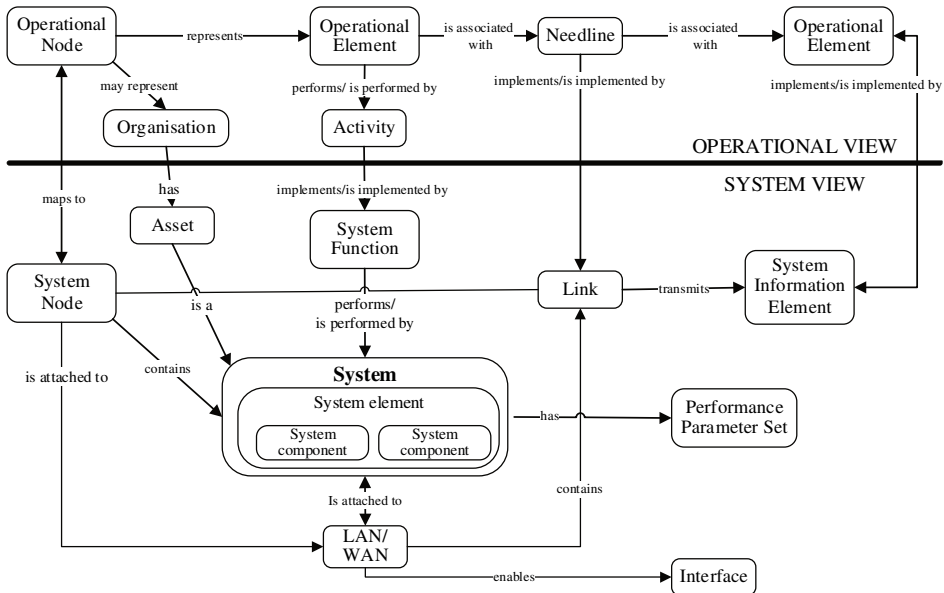


Fig. 2 High Level Data Information Metamodel of C4ISR V2.0 architectural framework

The operational architecture is intended to describe the tasks, operational elements and information flows necessary to perform or support the function of warfare. System architecture captures the flow of information between nodes, systems that support this stream, and communication systems that support networking. Local (LAN) and global (WAN) networks are specifications of architectural models and they relate to technical architecture. A system interface is a simplified or generalized representation of a communication path or network. Fig. 3 shows a conditional example of a description of the system interface of a military SoS C4ISR [7].

Fig. 3 reflects the organization of networks and the construction of military SoS, characteristic of that time very well. Today, such principles of SoS construction can be considered obsolete, but they have had a great influence on the formation of the NCW concept.

The development and use of new weapon systems require the creation of a new concept for their use. It can be said that the NCW concept was developed as part of the DoD C4ISR Cooperative Research Program (CCRP). The main challenge facing the CCRP was to improve the understanding by the US Department of Defense of the impact of the information age on national security. In July 2001, Congress held a hearing on the NCW [5]. Since that time, we can assume that this concept has become the basis for the development of the US armed forces, and later of NATO.

Definition of NCW can be read in [3]: “NCW is about human and organizational behavior. NCW is based on adopting a new way of thinking – network-centric thinking – and applying it to military operations. NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders’ intent”.

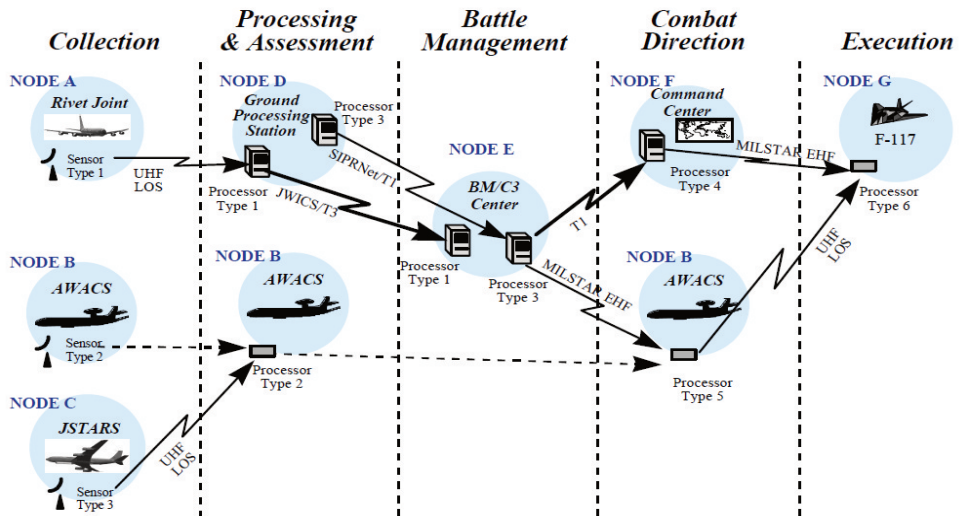


Fig. 3 A conditional example is the description of the system interface of the military SoS C4ISR, intermodal perspective (SV-1)

It should be agreed with the opinion of Darryn J. Reid [8] that the definition of NCW is vague and not specific. The key concepts somewhat concretize the definition of NCW [3]:

- the first key concept is the use of a geographically dispersed force,
- the second key concept is the fact that our force is knowledgeable,
- the third key concept is that there is effective linking achieved among entities in the battlespace.

The NCW basic tenets, formulated in [4], give some more information about the content of the concept:

- a robustly networked force improves information sharing,
- information sharing and collaboration enhance the quality of information and shared situational awareness,
- shared situational awareness enables self-synchronization,
- these, in turn, dramatically increase mission effectiveness.

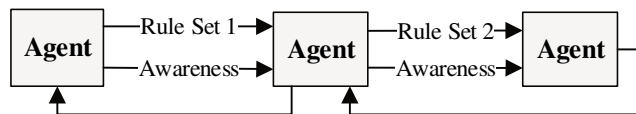
Note that NCW, as a scientific concept, is very vulnerable to criticism. The criticism of the NCW from a philosophical point of view contained in [8] is very interesting in this matter. The validity of this criticism is confirmed by the fact that its provisions are presented in a report to Congress [12].

The authors of the NCW concept note that NCW is based on adopting a new way of thinking – network-centric thinking – and applying it to military operations [3]. Yes, a revolution in military affairs requires new thinking. And here Darryn J. Reid notes that in many ways the approaches of the NCW authors are similar to the scientific cognition of Sir Francis Bacon, characterized by objective observation, inductive generalization, empirical justification, and deductive prediction, which is now called “inductivism”.

Inductivism is intuitively seductive; Bacon opened his inductivism religion with the promise of knowledge and power to those who followed its method, and similarly, NCW promises almost unlimited improvements in combat power through the use of digital networks [8]. Moreover, the authors of NCW intentionally or unintentionally primitivize warfare: “The key to understanding the roles of and the relationships among battlespace entities is to focus on processes that turn raw data into information, and information into knowledge” [3]. Controlling the behavior of complex systems is largely reduced to self-synchronization, and even the very concept of “self-synchronization” and its argumentation are quite controversial.

Self-synchronization is considered as a way of interaction between two or more entities [3]. Fig. 4 [3] shows the key elements of self-synchronization. It is assumed that general awareness and a set of rules that determine the desired result in various operational situations which allow entities to act effectively in the absence of traditional hierarchical mechanisms of command and control.

The paradox of self-synchronization is that the circuit itself shown in Fig. 4, hierarchical, and the process of self-synchronization, according to the same authors, is not global, but limited in nature: “There are certain types and kinds of relationships that by their nature do not lend themselves to self-synchronization and others where the application of self-synchronization can yield significant benefits. An area where the application of self-synchronization has significant potential is a class of warfighting activities providing supporting services, such as logistics, fire support, and close air support” [3].



*Fig. 4 Self-Synchronization Interaction*

The decisions and actions of commanders of various ranks must of course be coordinated and synchronized. But this synchronization has little in common with the declared principles of self-synchronization. From the point of view of military science, statements about massing effects instead of massing forces are quite controversial [3].

Making intermediate conclusions, it should be noted that the idea of NCW itself is absolutely consonant with the idea of a revolution in military affairs, which predetermined its wide distribution. The concrete implementation of this idea is criticized. We believe that the thesis of “networking leads to improved performance” is false. Networking is a necessary but not sufficient condition for increasing productivity. It creates only the conditions for the further integration of individual network elements into target systems that are optimized to achieve specific goals.

### **3 The Impact of Destructive Technologies on the Development of the NCW Concept and Military Architectural Frameworks**

The C4ISR architectural framework turned out to be a very convenient marketing tool for monitoring the development and acquisition of the system by government managers at all stages [13]. This predetermined the further creation of AF on its basis for the ministries of defense of various countries and the NATO block. However, there

were certain difficulties along the way. C4ISR AF was product-oriented and not suited for creating large-scale software-intensive systems.

In May 2003, the US Department of Defense adopts the Net-Centric Data Strategy (NCDS) [14]. NCDS considers the goal of making data assets visible, accessible, and understandable to various end users as a primary goal. Fig. 3 shows that for the exchange between the individual systems included in the SoS, certain interfaces are used that are adapted for these systems. The problem arises of creating mechanisms that provide access for various users to information (Fig. 5) [15].

In February 2004, DODAF 1.0 was released. The first versions of DODAF as a whole can be considered as a further development of C4ISR AF, however, the scope of DODAF was expanded beyond C4ISR and now covers all areas of activity of the US Defense Ministry. The approach to products has become more data-oriented.

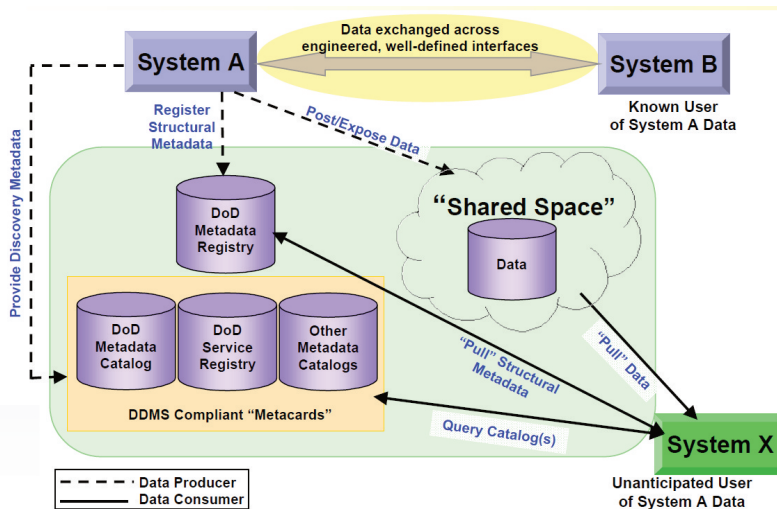


Fig. 5 NCDS enables unanticipated users [15].

The development of high-precision weapons (RMS less than 10 m) led to the fact that the accuracy of hitting a target began to be determined not by the capabilities of high-precision munitions, but by the capabilities of reconnaissance and control systems for high-precision determination of target coordinates. For example, the high accuracy of determining the coordinates of targets is practically unattainable using paper topographic maps, and even satellite systems do not always provide the required accuracy [16]. All this leads to the fact that the task of combining data from various sources is transformed into the problem of the interaction of heterogeneous systems to obtain the necessary data.

The ongoing changes in the development of the armed forces require their understanding and in March 2007 the US Congress listens to the report "Network Centric Operations: Background and Oversight Issues for Congress" [12], which considers both the positive and negative aspects of the NCW concept. It is characteristic that instead of NCW, a new terminology began to be used: "Network Centric Operations is a theory which proposes that the application of information age concepts to speed communications and increase situational awareness through networking improves both the efficiency and effectiveness of military operations" [12].

The development of network technologies has led to the fact that in April 2007 DODAF 1.5 (Fig. 6) was released, which implies the widespread use of service-oriented architecture.

In developing this trend, in May 2007, the United States Department of Defense released a document entitled: “Strategy for a Net-Centric, Service Oriented DoD Enterprise”, which made the following statement: “Changes in the network-centric strategy of the United States Department of Defense reflect the recognition that a service-oriented approach can lead to explosive opportunities for our fighters and decision makers, and thereby increase operational efficiency”. Net-Centric Services Strategy (NCSS) addresses the challenge of developing services which makes it easier for consumers to use information resources and access to data. US Department of Defense is to create a Net-Centric Environment (NCE), which increasingly uses common services and service-oriented architecture (SOA) [17].

In 2009, the second version of DoDAF V2 + was released, which directly declared the change from “product-centric” to “data-centric” methodology [18]. It is emphasized that data is a key point in the development of architecture, providing integration and interaction between different architectures within the framework of heterogeneous architectural methodologies. The main emphasis has been shifted to the methods of collecting, systematizing and analyzing data on architecture based on a common data metamodel. This leads to a fundamental change in AF. In fact, it is recognized, but not declared, that if in the 90s of the last century the main task was to combine dissimilar weapons and military structures into a single network, then at present such a problem has already been solved and further development is possible through effective use of data-centric technology.

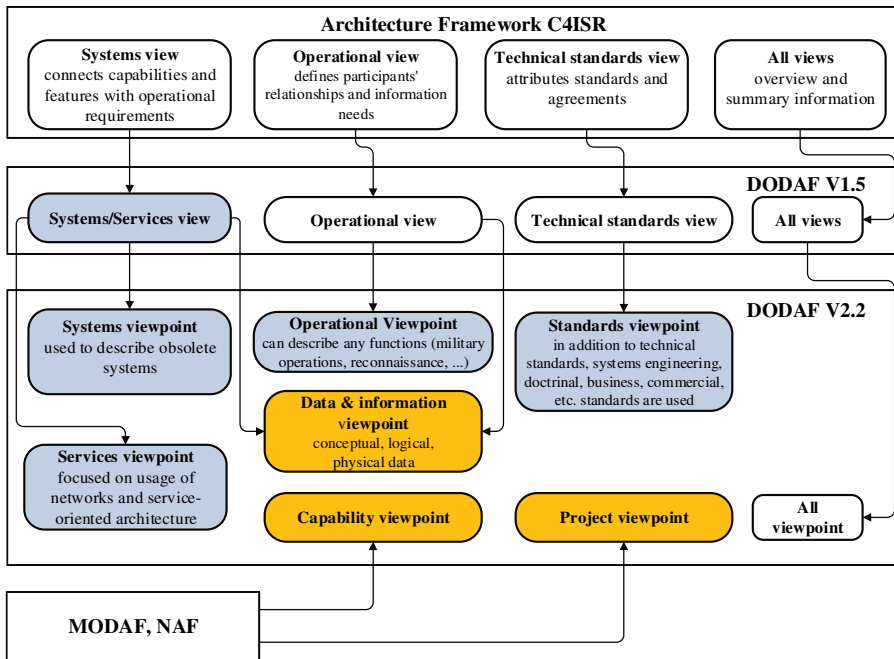


Fig. 6 The development of architectural frameworks of the United States of America



The development of data-centric technologies leads to the fact that in a single network, the influence of the peculiarities of the systemic construction of one or another weapon sharply decreases. Similarly, systems with different software and various hardware platforms interact on the Internet without problems. Therefore, in DODAF 2.02, Systems, Viewpoint (Fig. 6) is used only to describe obsolete systems. The significant development of “system engineering” predetermined the “migration” of new methods for describing “Capability” and “Project” in DODAF 2.02 from the architectural frameworks of NATO (NAF) and the United Kingdom of Defense (MODAF), which further emphasizes the possibilities and not the requirements for SoS design. But the most important thing was the use of the new Data & Information viewpoint.

One effective way to deal with complexity is to use abstraction. Data & Information viewpoint includes three levels of abstraction: conceptual, logical and physical.

The use of data-centric technologies required a common understanding of various entities not only by specialists in various fields, but also by systems with artificial intelligence (Artificial Intelligence – AI), which inevitably led to a close look at ontology issues. Initially, the question for AI developers was: how to describe the world so clearly that even a computer can interpret these descriptions [19]. There is a reference to the statement by Tom Gruber, who formulated a new definition of ontology: “Ontology is a formal specification of a shared conceptualization” [19].

The International Defense Enterprise Architecture Specification (IDEAS) proposed a formal ontology that facilitates the interoperability of architecture models [18]. The IDEAS ontology was the basis for the DODAF data metamodel, and was later extended to other AF of NATO countries.

If in AF C4ISR the main resource was information, then in AF, based on the IDEAS ontology, the list of used resources is expanded. This is a very important point. Now the operation is carried out not only by information flows, but also by Item flow. That is, exchange is globalizing, flows can now be understood not only as information, but also as other resources, for example, materials and energy.

Such an expanded representation of flows was accompanied by an exponential increase in the number of devices connected to the network. The Internet of Things (IoT) arises [20]:

“We are now in the midst of enormous technological change. And, there are huge risks and opportunities associated with this change... IoT is extending the reach of the Internet to inexpensive, miniature, pervasive computing and control devices”. IoT is seen by the military as a disruptive technology [21]. It is quite obvious that this technology immediately got its military direction - Internet of Battlefield Things (IOBT) and had its impact on C3I [22].

In December 2018, the US Department of Defense released a document called: “DoD Cloud Strategy” which focuses on the fact that in the modern era of military operations, the battlefield exists not only in the physical, but also in the digital world [23]. Cloud technology is a fundamental component of global infrastructure and is critical to maintaining the technological advantage of the U.S. military in warfare during the 21<sup>st</sup> century. Cloud computing is a service that provides network storage and computing resources. It allows users to access information from anywhere at any time, effectively eliminating the need for the user to be in the same physical space as the hardware on which the data is stored [23].

IoT and cloud technologies have led to the rapid development of unmanned systems and AI. Artificial systems acquire their own behavior, previously characteristic only of living systems. The role of AI is so growing that DOD is developing an “artificial intelligence strategy” [24].

The battlefield expands to cyberspace. In April 2015, the DOD Cyber Strategy was adopted, and in June 2018, the Joint Chiefs of Staff (CJCS) adopted joint doctrine to plan, execute, and assess cyberspace operations [25].

Further development of a single information-combat space is associated with the development of the Federated Mission Networking program.

Federated Mission Networking is a capability aiming to support C2 and decision-making in future operations through improved information-sharing. It provides the agility, flexibility and scalability needed to manage the emerging requirements of any mission environment in future NATO operations.

As an intermediate conclusion, we note that the military revolution [6], which became the basis for the development of the NCW concept, was based on the 3<sup>rd</sup> industrial revolution, caused by the development of semiconductors, computers and the Internet. At present, the 4<sup>th</sup> industrial revolution is underway, which is introducing revolutionary changes in the military field, and requires the development of new concepts for constructing weapons and conducting military operations. The accumulated destructive technologies lead us to the next bifurcation point, the way out of which is associated with the development of a new Data-Centric Warfare concept and the development of data-centric weapon systems.

#### 4 The Data-centric Operation Theory and Data-centric 4D Architecture

Data-centric weapon systems can be considered as the result of the development of a general theory of systems in the field of building complex systems and information technologies. Fig. 7 shows the innovations and technologies that formed the basis for creating the theory of data-centric operations.

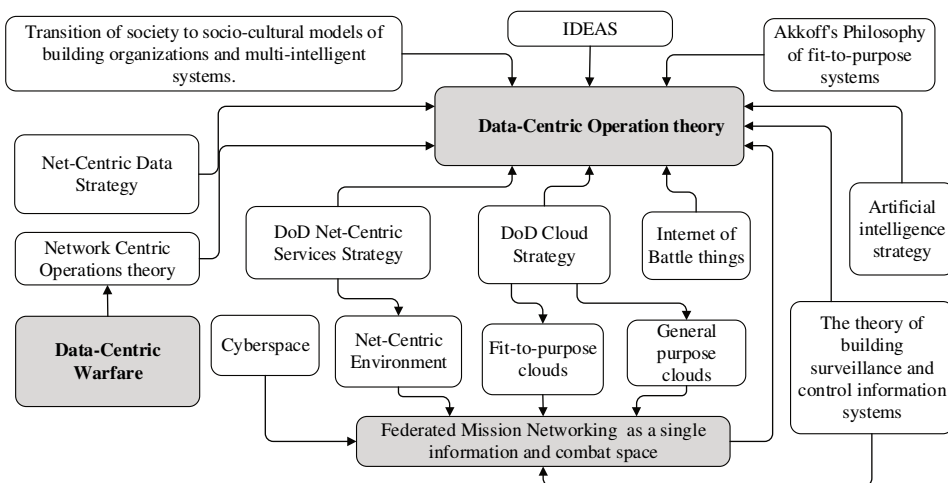


Fig. 7 Innovations and technologies that formed the basis for creating the theory of data-centric operations

The interaction of individual systems within a single system of systems can be adapted to provide the desired capabilities depending on the situation. At the same time, a situation often arises when functions that are redundant during the operation of a separate weapon system as part of SoS may be required for autonomous combat operations. Currently, the military are not ready to abandon the hardware redundancy of their systems, given their very possible autonomous work outside SoS. The presence of hardware redundancy during the operation of individual weapon systems as part of SoS makes the task of using these resources to obtain additional capabilities and increase the effectiveness of SoS as a whole relevant.

The complication of the organization of any artificial objects is carried out within the framework of the chain: aggregation - networks - systems. The property of system integrity is determined by the unambiguous allocation of a subset of system elements from network elements localized spatially and chronically.

Chronical localization of the system is determined by the fact that achieving the goal can be carried out in several stages, at which the tasks of the system, and therefore the set of system functions and the set of elements necessary for the implementation of these functions, can change. With this approach, the structure of data-centric SoS (DSoS) is determined by the trajectory of its substitutional movement (SM), by the set of stable states, and relations between them during the functioning of the system to achieve its goal.

The substitutional movement of the system (“substitutio (lat.)” means “replacement”) is the process of replacing its elements at one or more levels of its hierarchical structure. The environment for DSoS is the network. With a “system-centric” point of view, the input of a “fixed” system receives item flows, the replacement of items takes place, that is, the course of the substitutional time of the system.

The DSoS can be defined as: isolated spatially, limited chronically, changing in time and relatively self-sufficient fragment of the world and organized integrity, consisting of parts, united by various relations, which has a common special quality (emergence), not equal to the sum of properties, parts of this whole. DSoS information communications are well described using the metamodel for the UML profile for DoDAF and MoDAF shown in Fig. 8 [26].

For the DSoS metamodel, it is characteristic that, in contrast to the C4ISR information model (Fig. 2), the operation of operational nodes is much less associated with the construction features of individual system nodes, and the variability of the structure is described using entity flows (Item flow).

The current structure (time slice of 4D-space) is determined by the capabilities required for the current time interval (Capability). Thus, DSoS can be considered both as a fit-to-purpose systems and as network resources.

A new quality in data-centric systems is configuration management through the optimal use and distribution of network resources over time. Data-centric systems change their structure not only due to their own resources, but due to the dynamic linking of network resources as part of the tasks performed by the system for a given period of time.

To achieve the goal, it does not matter what the system consists of, but it is important what it can do. In any case, the ability to fulfill the goal determines the system. Consequently, the system is determined not by the composition of its elements, but how accurately it can fulfill what is expected of it. What matters is the



The next important issue is the separation of the system and the external environment from the point of view of management. And in this regard, it would be worthwhile to turn to the thoughts expressed by J. Gharajedaghi. The concept of the external environment includes all variables that affect the behavior of the system, but are not subject to its control. Thus, the boundary of the system becomes a conditional and subjective component, established on the basis of the capabilities or powers of management. However, there are parameters not subject to our control, but subject to our influence. Management involves an action that is necessary and sufficient to obtain a result. Influence means that the action is not a sufficient condition – it only contributes to the achievement of the result [27].

This is a very important point for us. The development of network technologies has given rise to an “era of information” and the ability to effectively implement Alfred Stone’s management model, based on a biological (mono-intelligent) system organization model [27]. In fact, most large companies and military organizations began to use this model. But there is the famous saying “victory changes the rules of the game”. A paradigm shift has taken place and the competitive advantage is increasingly shifting from the NCW concept to the data-centric. The transition to a data center is accompanied by a change of the biological model of organizing systems to a multi-intelligent system.

One of the most important issues in the formation of the theory of data-centric operations is the use of “system-system thinking” or by the definition of Akoff: “the model thinking” [27]. It should be noted that the very concept of system has developed along with the development of systems thinking. The first generation of systems thinking solved the problem of interdependence in the context of mechanistic (deterministic) systems. The research of operations was the predominant area of systems thinking [27].

The second generation of systems thinking (cybernetics and open systems) dealt with a double problem: interdependence and self-organization (negentropy according to Ackoff) in the context of biological or mono-intelligent systems. It is this generation of systems thinking which is associated with the theory of network-centric operation – increasing interdependence by “linking” individual participants in the network and “self-synchronization” as a variant of self-organization.

The third generation (model thinking) is currently trying to cope with a triple problem: interdependence, self-organization and choice. And the developers of the model are trying to choose (design) rather than predict the future. The effectiveness of a multi-intelligent organization depends not so much on the management of the actions of its members, but on the management of their interactions [27]. It is the third generation of systems thinking which determines the development of data-centric systems-systems that implement the paradigm: “interdependence, self-organization and choice”.

The theory should fully explain the known facts, bringing them under the system of relations-laws, which are defined as those that underlie them. “Theory, also, is a hypothesis accepted for argumentation or research, unproven assumption”, the formulation of obvious relationships or basic principles of certain observed phenomena that have been tested to some extent.

NCW's working hypothesis is that the armed forces in which network support is implemented for all organizational forms and processes – the networked forces have an advantage over the traditional ones.

The theory of data-centric operations assumes (the main hypothesis) that the application of key factors of the 6<sup>th</sup> technological order increases both efficiency and effectiveness of operations due to the transition to the paradigm of multi-intelligent systems based on socio-cultural model, dynamic reconfiguration of target system and operating environment systems, depending on changing environmental conditions.

The theory of data-centric operations is based on the five concepts:

- metamorphism – variability & agile development,
- 4D extentionalism,
- dualism of DSoS,
- interoperability due to data integration,
- co-evolution and eco-systems created around the target system.

The concept of interoperability of data-centric systems should be considered primarily as an opportunity to integrate systems based on data integration within a common network in contrast to system integration at the physical level.

The concept of co-evolution has been transferred from biological systems to DSoS. It considers the co-evolution of the target system, life cycle support systems and operating environment systems as a single eco-system created around the target system.

## 5 Conclusions

At the present stage, the front-end of systems engineering are Network intensive systems. Even more complex systems are data-centric systems and other systems with organizational governance.

Fundamental concepts of constructing weapons systems are changing radically, and the boundaries between individual weapons systems and their operational environment are becoming less clear. The increasing complexity and interdependence of systems, the development of SoS and FoS, and their structural variability caused a significant increase in the role of architectural approaches in the design of weapons.

Today's vision of network-centric warfare is significantly different from what was originally invested in this concept. The combination of IDEAS ontology, SOA and cloud architecture, supported by the modern development of unmanned systems, AI, IOBT and communication systems, creates disruptive technology that should fundamentally change the concept of warfare.

The DCOT is based on a 4D-extensional representation of the combat space of weapon systems integrated into a single network. Many armament samples connected by a network occupy some 3D space. Assembling a cluster system to perform a specific function/task is carried out dynamically in real time. Therefore we can say that the current structure of the system is defined as a section of 4D space by the time plane. Events are three-dimensional “slices” at specific time points in the life of a data-centric system.

## References

- [1] CLAUSEWITZ, C. *On War*. New Jersey: Princeton University Press, 1989. ISBN 978-0-691-01854-5.
- [2] CHRISTENSEN, C.M. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston: Harvard Business Review Press, 2016. ISBN 978-1-63369-178-0.

- 
- [3] ALBERTS, D.S., J.J. GARSTKA and F.P. STEIN. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2<sup>nd</sup> ed. Washington: CCRP Publication Series, 1999. ISBN 978-1-57906-019-0.
- [4] ALBERTS, D. and R.E. HAYES. *Power to the Edge: Command and Control in the Information Age*. Washington: CCRP Publication Series, 2005. ISBN 978-1-893723-13-9.
- [5] *Network Centric Warfare* [online]. July 2001 [viewed 2020-05-03]. Available from: [http://www.dodccrp.org/files/ncw\\_report/report/ncw\\_cover.html](http://www.dodccrp.org/files/ncw_report/report/ncw_cover.html)
- [6] OWENS, W.A. *The Emerging U.S. System-of-Systems* [online]. February 1996 [viewed 2020-05-03]. Available from: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a394313.pdf>
- [7] *C4ISR Architecture Framework Version 2.0* [online]. December 1997 [viewed 2020-05-12]. Available from: <https://www.afcea.org/education/courses/archfwk2.pdf>
- [8] REID, D.J., G. GOODMAN, W. JOHNSON and R.E. GIFFIN. All That Glisters: Is Network-Centric Warfare Really Scientific? *Defense & Security Analysis*, 2005, **21**(4), pp. 335-367. DOI 10.1080/1475179052000345403.
- [9] SKORYK, A., I.G. KIRILLOV and K.A. TURSUNHODZHAEV. About Methodology of an Estimation of Influence of Complexity of Structure of Military-Technical Systems on Fighting Potential of Military Formations (in Ukrainian). *Systems of Arms and Military Equipment*, 2010, **4**(24), pp. 237-241. ISSN 1997-9568.
- [10] *C4ISR Architecture Framework Version 1.0* [online]. June 1996 [viewed 2020-05-12]. Available from: <https://fas.org/irp/doddir/dod/c4ISR/index.html>
- [11] LEVIS, A.H. and L.W. WAGENHALS. C4ISR Architectures: I. Developing a Process for C4ISR Architecture Design. *Systems Engineering*, 2000, **3**(4), pp. 225-247. DOI 10.1002/1520-6858(2000)3:4<225.
- [12] *Network Centric Operations: Background and Oversight Issues for Congress* [online]. March 2007 [viewed 2020-05-12]. Available from: <https://www.everycrsreport.com/reports/RL32411.html>
- [13] WOOD, W.G. and S.G. COHEN. *DoD Experience with the C4ISR Architecture Framework* [Technical Note] [online]. September 2003 [viewed 2020-05-12]. DOI 10.1184/R1/6573293.v1. Available from: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6527>
- [14] *DoD Net-Centric Data Strategy* [online]. May 2003 [viewed 2020-05-12]. Available from: <https://dodcio.defense.gov/Portals/0/Documents/Net-Centric-Data-Strategy-2003-05-092.pdf>
- [15] RIOFRIO, H.J. *U.S. Department of Defense (DoD) Net-Centric Data Strategy* [online]. October 2004 [viewed 2020-05-07]. Available from: <http://sesam.smartlab.se/seminarier/hostsem04/HJR.pdf>
- [16] SKORYK, A., O. FLOROV, Y. MORHUN, D. MOLCHANOV, O. HRECHKA and S. SHEPELEVYCH. Analysis of the Features of Construction and Using of Perspective Control Systems of the High-Precision Weapons (in Ukrainian). *Positioning systems, Science and Technology of the Air Force of Ukraine*, 2018, **4**(33), pp. 43-51. DOI 10.30748/nitps.2018.33.06.

- 
- [17] *DoD Net-Centric Services Strategy* [online]. March 2007 [viewed 2020-05-12]. Available from: [https://dodcio.defense.gov/Portals/0/documents/DoD\\_Net\\_CentricServicesStrategy.pdf](https://dodcio.defense.gov/Portals/0/documents/DoD_Net_CentricServicesStrategy.pdf)
- [18] GIACHETTI, R.E. Evaluation of the DoDAF Meta-model's Support of Systems Engineering. *Procedia Computer Science*, 2015, **61**, pp. 254-260. DOI 10.1016/j.procs.2015.09.208.
- [19] LEVENCHUK, A. Systems Engineering Thinking (in Russian) [online]. April 2015 [viewed 2020-05-20]. Available from: [https://techinvestlab.ru/files/systems\\_engineering\\_thinking/systems\\_engineering\\_thinking\\_2015.pdf](https://techinvestlab.ru/files/systems_engineering_thinking/systems_engineering_thinking_2015.pdf)
- [20] *DoD Policy Recommendations for the Internet of Things* [online]. December 2016 [viewed 2020-05-20]. Available from: <https://www.hsd1.org/?view&did=799676>
- [21] TONIN, M. *The Internet of Things: Promises and Perils of a Disruptive Technology* [online]. October 2017 [viewed 2020-05-20]. Available from: <https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017-+-175+STCTTS+17+E+bis+--INTERNET+OF+THINGS.pdf>
- [22] RUSSELL, S. and T. ABDELZAHER. The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making. In: *Proceedings of the MILCOM 2018 – 2018 IEEE Military Communications Conference (MILCOM)*. Los Angeles: IEEE, 2018, pp. 737-742. DOI 10.1109/MILCOM.2018.8599853.
- [23] *DoD Cloud Strategy* [online]. December 2018 [viewed 2020-05-20]. Available from: <https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF>
- [24] TARRAF, D.C., et al. *The Department of Defense Posture for Artificial Intelligence. Assessment and Recommendations* [online]. Santa Monica: RAND Corporation, 2019 [viewed 2020-05-20]. ISBN 978-1-9774-0405-3. Available from: [https://www.rand.org/pubs/research\\_reports/RR4229.html](https://www.rand.org/pubs/research_reports/RR4229.html)
- [25] *Cyberspace Operations* [online]. June 2018 [viewed 2020-05-12]. Available from: [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf)
- [26] HUE, M. *An Analysis of SE and MBSE Concepts to Support Defence Capability Acquisition* [online]. Edinburgh: Defence Systems Integration Technical Advisory, 2014 [viewed 2020-05-12]. Available from: <https://apps.dtic.mil/sti/pdfs/ADA624596.pdf>
- [27] GHARAJEDAGHI, J. *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*. 3<sup>rd</sup> ed. San Francisco: Morgan Kaufmann, 2011. ISBN 978-0-12-385915-8.