The 13th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 8th-9th 2018

COLLABORATIVE COMMUNICATION AND INFORMATION SYSTEM IN MODERN THEATRES OF OPERATIONS

Manuel Florin ONOFREI

Ministry of National Defence/ Romania

Abstract:
In modern theatres of operations there is a spectacular increase in the unconventional dimension of conflicts, the armed conflict being mostly informational, and the informational war constitutes a component worthy of consideration by any strategist who wants to win. The current situation and the trends in the US and NATO for the implementation of a collaborative communication and information system used in modern theatres of operations will be briefly presented in this article. We will also emphasize the importance of the architectural framework in the organization, integration and usage of collaborative communications and information systems in the modern theatres of operations

Key words: collaborative, communication and information system, enterprise architecture, Department of Defence Architecture Framework (DoDAF), NATO Architecture Framework (NAF), Network Centric Warfare (NCW), Federated Mission Networking (FMN) .

1. Introduction

Modern contemporary conflicting actions are recognized as Network Centric Warfare (NCW) actions by most military specialists (David S. Alberts, John J.Garstka, Alvin Toffler etc.). Through the notion of "warfare" they seek to frame a military action between two elements antagonistic, without strictly framing it in the military norms of the dimensions of space and time, according to the Clausewitz model, by which the categorization of military actions was established as: at strategic level-the war, at operational level-operations, and at tactical level-battles. In other words, the notion "warfare" assumes any of these three types of actions listed above, following to clarify the level of action will by the content of this article.

2. Considerations on evolution trends in modern theatres of operations

Modern armed conflicts are perceived more as a continuation of policy with other means, in the light of the fact that it represents a confrontation between social, political, economic, diplomatic, ideological, psycho-moral and informational components. These include, in general terms, confrontations from different fields and backgrounds, which have their own laws and principles, causing an alteration of the classical war forms and processes, a specific organisation and a strict specialization of the forces and means, limiting human losses and increasing the role of political-military-ideological threats. [1]

The peace and war are no longer separated in the modern theatres of operations, because peace coexists with war, nonviolent means and actions are used more and more often, and the major clashes are in the information zone. Although they are found in a vast

space represented by the areas of interest of the big powers and are carried out over a long period of time, the continuity of these is evident. [2]

In the future, in theatres of operations will participate over-technologized and informational entities, in order to obtain information supremacy, and the confrontation of the violent army, with loss of life and material destruction will be put under control or it will disappear. The conflict will eventually become, an instrument or a means of the international community crisis management policy that exists at a specific given time. In this respect, the policy of modernisation of the armies will be continued, the professional armies and their international components shall be developed, and the confrontation will be carried out largely by ultra perfected, intelligent, selective and high efficiency means. [3]

The main elements of the evolution of employment levels from the classic war to modern war are presented in *figure no. 1*

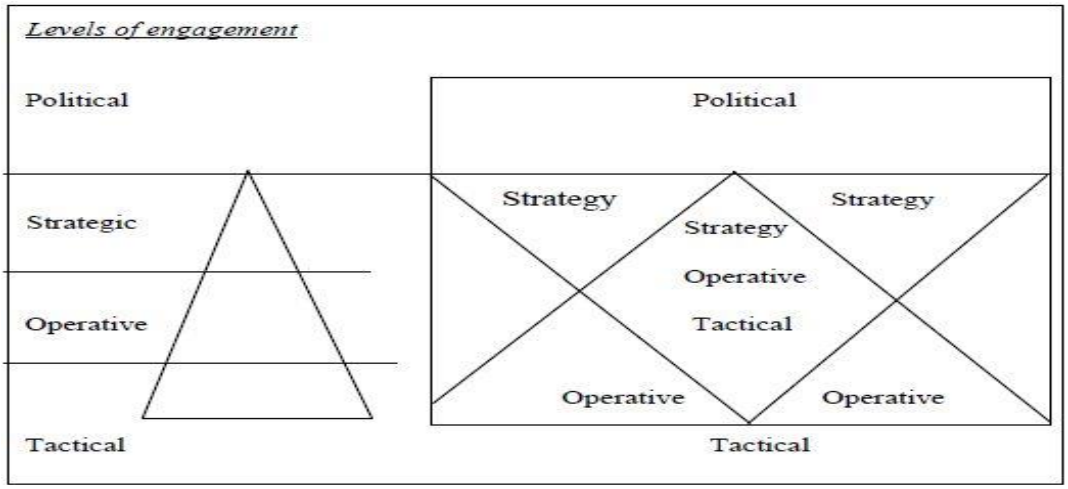

Figure 1. Evolution of the levels of engagements from the classic war to modern war (https://www.wikipedia.org)

Actions specific to modern theatres are carried out in a multidimensional space where informational, cyber and electromagnetic spaces complement the three-dimensional terrestrial, air and sea space, specific to the classical theatres of operations. [4]

We are currently in a transitional period from the classical, interstate theatre of operations, to the modern theatre of operations, in which new features are added, such as: asymmetry, flexibility, multilateralism, different intensity and demilitarisation. [5]

Communication and information systems are inevitably in a transitional period from non-cooperative-linear communications and information systems, specific to the classic theatre of operations to collaborative communications and information systems, specific to the modern theatre of operations. [6]

3. The place and role of architecture framework in the development of the military organisations

Architecture is generally understood as the science and art of designing and building, according to certain proportions and rules, determined by the character and destination of the final result. Arranging all component elements within an organization defines its architecture. The *Enterprise Arhitecture (EA)* is an asset that can lose value if it is not updated. Some parts of the EA do not change very often. We outline that the architecture elements such as mission, objectives, and capability do not change often once a goal has been established. This rate of change is consistent with the relative stability of WHAT an enterprise does. HOW the

enterprise does what it does may change from time to time based on reorganization, continuous improvements, re-engineering process and constant assessment of best practices to name a few factors. The key to the information age is architecture. The information age is characterized by the focus on groups of people collaborating in pursuit of a common mission or purpose—that is, on enterprises. [7]

When we are speaking about architectures, we are speaking about the means of achieving high-level objectives, either within NATO or within the member states. A common approach to architecture is considered to be the best way to achieve success in developing a federation of systems with the aim of facilitating a future network-based paradigm in a service-based architecture. In DoDAF enterprise there are three basic levels of architecture usually used, the Enterprise, the Segment, and the Solution. These three levels are illustrated in *figure no. 2*

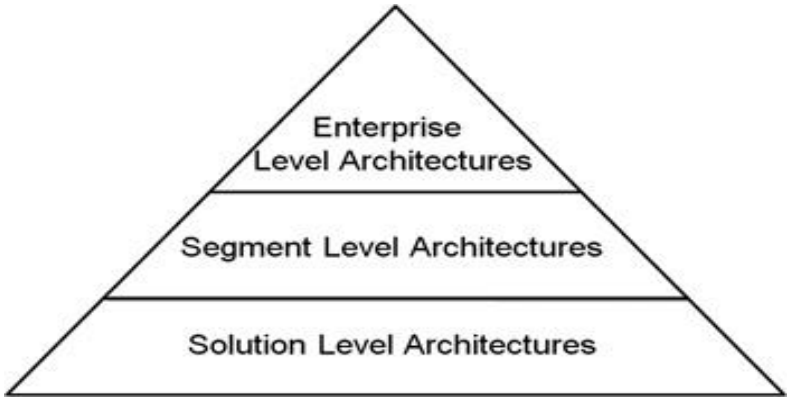

Figure 2 Levels of DoDAF enterprise architectures [11]

An architecture framework establishes a set of terms that describe the various types of architecture elements. For example, Department of Defence Architecture Framework (DoDAF), defines architecture elements such as activity, performer, location, and capability. The use of a single architecture framework across an enterprise means that all the architects will be using the same set of well-understood terms. Details of the concepts used at the level of an organisation and the relations between them, in *figure no. 3*

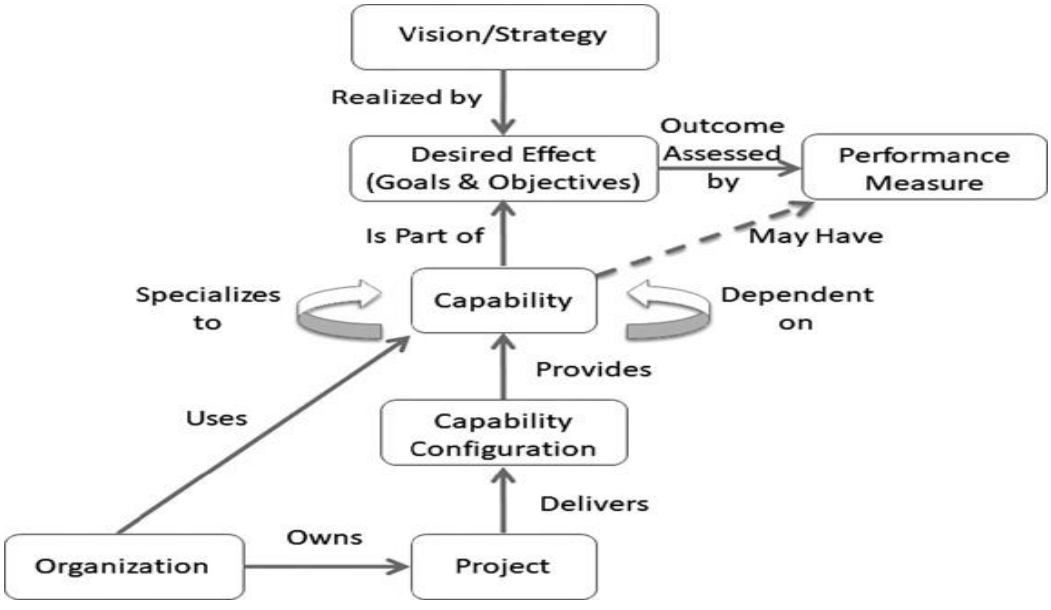

Figure 3 Enterprise Level domain concepts and relationships [11]

In the past decades, discoveries, learning, and knowledge have been borrowed from one to another between the military of the United States (*DoDAF*), Canada (Department of National Defense/Canadian Armed Forces Architecture Framework - *DNDAF*), United Kingdom (United Kingdom's Ministry of Defense Architecture Framework -*MODAF*), Australia (Australian Defense Architecture Framework - *DAF*), and the North Atlantic Treaty Organization (North Atlantic Treaty Organization Architecture Framework - *NAF*). An overview of Enterprise Architecture Frameworks evolution is ilustrated in *figure no.4.*

Efforts are currently underway to specify unified architecture framework ontology based on this defense architecture frameworks with assistance from standards bodies such as the Object Management Group (*OMG*).

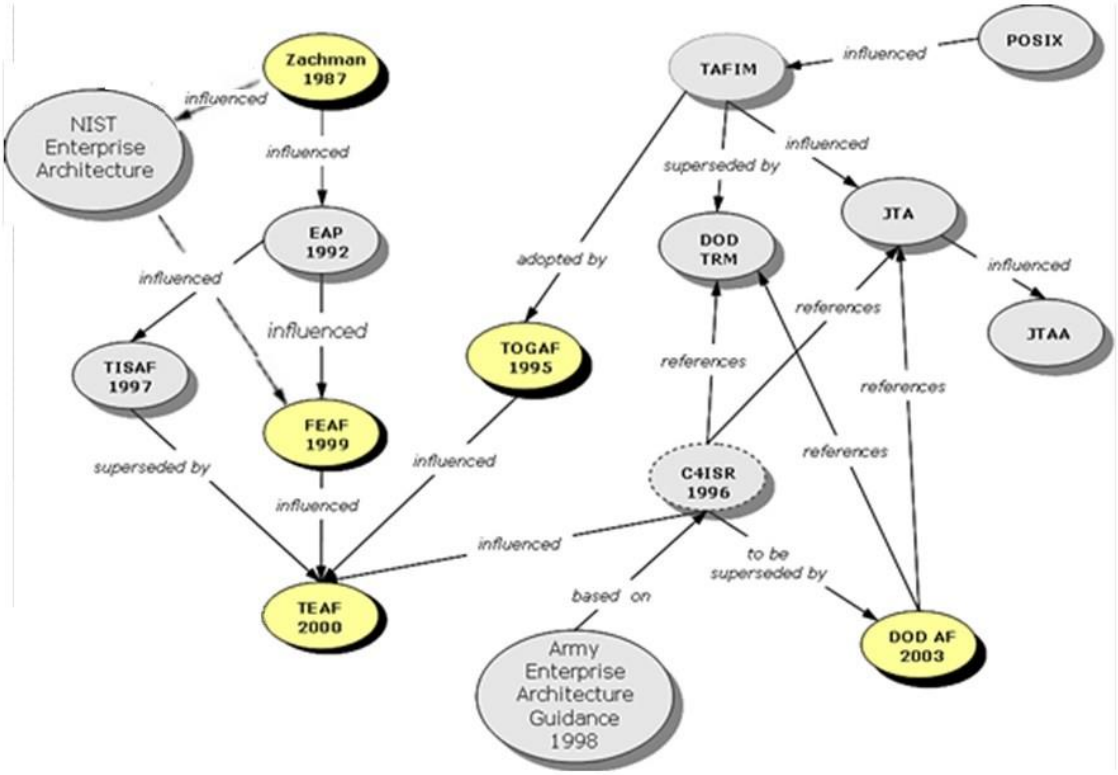

Figure 4 Overview of Enterprise Architecture Frameworks evolution (1987–2003) (https://www.wikipedia.org)

4. The place and role of collaborative communications and information systems in modern theatres of operations

The information underpinnings the operation of any integrated command and control system. They are growing continuously, both in importance and in volume, and contain data relating to the adversary, their own troops, the battle space and events that influence the deployment of military actions. Following automatic processes of processing, analysis, storage and recovery, this information ensures the base of commander's decision. [9]

The collaborative communication and information system integrates all networks and services to optimise the organization's activities and processes by reducing transmission time, efficient management of information flows, and eliminating the dependency on equipment. The collaboration is accomplished by ensuring the implementation of the requirements imposed on the network and services, namely: convergence, integration,

digitalisation, interoperability, standardization, virtualization, quality of service, architecture oriented services etc.

The implementation of collaborative communication and information system is favoured by a number of new requirements, as following: representing data in the same format, developing technologies that allow for increased processing power, storage capacity, transmission speed, data compression and correction of errors; favouring the processing, recording and transmission of messages easily; developing universal IP standards and migrating networks to this technology; use of data compression methods leading to increased transmission capacity of communication channels; expanding and generalizing data transmissions via IP-based packet switching. In this context, we believe that the collaborative communication and information system in the modern theatres of operations must be developed up to the fighter level, whose architecture is consistent with NAF, and framework architecture must be used as an analysis tool for developing new capabilities, optimizing collaborative communication and information system processes and associated costs.

5. Collaborative communication and information system used in modern theatres of operations by the US

The DoDAF it was used as the basis for many other defence frameworks and its views are compatible with the TOGAF and form a subset of the Federal Enterprise Architecture Framework Version 2 (FEAF2) views. General terms of the defence architecture frameworks enable them to be equally easily applied to developing weapons systems as to developing force structures and military missions and operations during wartime and peacetime. The need for coalition partners to interoperate and collaborate during coalition operations also requires that military partners have comparatively consistent, interoperable and well-documented architectures. [9]

The primary purpose of DoDAF was to provide a common format and semantics for comparison, aggregation, and analysis of U.S. Navy, U.S. Army, U.S. Air Force, U.S. Marine Corps, and the U.S. Coast Guard architectures. With a common framework, classes of complex problems in a theatres of operations or on the battlefield such as joint asset visibility, joint mission threads, common operating picture, and others can be tackled by federating multiple architectures during the planning, acquisition, and resourcing phase to ensure that collaboration, interoperability, single operating picture, and unity of actions are accomplished under critical war-fighting conditions. One of the most important needs met by the DoDAF was an integrated view of architecture elements through many views that share subsets of the same architecture elements. (f*igure no. 5*)

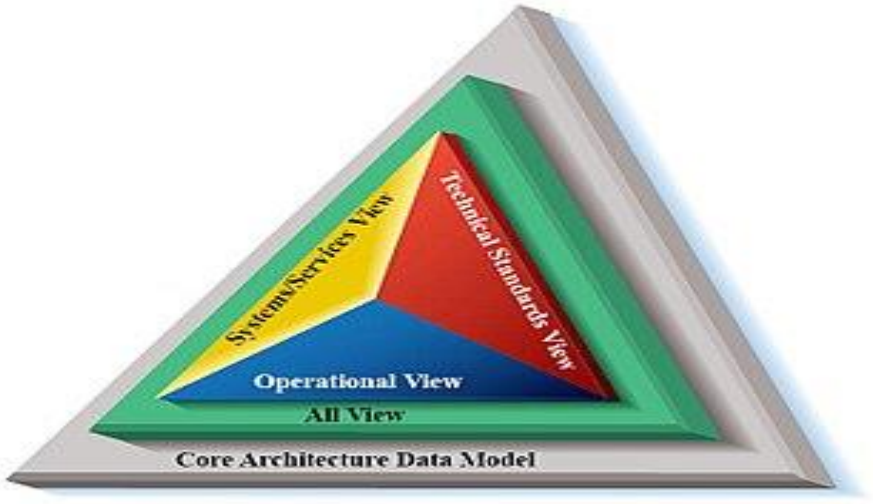

Figure 5 DoD Architecture Framework v1.5 (https://www.wikipedia.org)

Work on DoD's Intelligence, Surveillance, and Reconnaissance (ISR) project started in the mid-1990s, with trying to compare the architectures proposed by various contractors in response to DoD requests. Along time, ISR evolved into the DoD C4ISR Framework and became lately the DoDAF. (f*igure no. 6*)

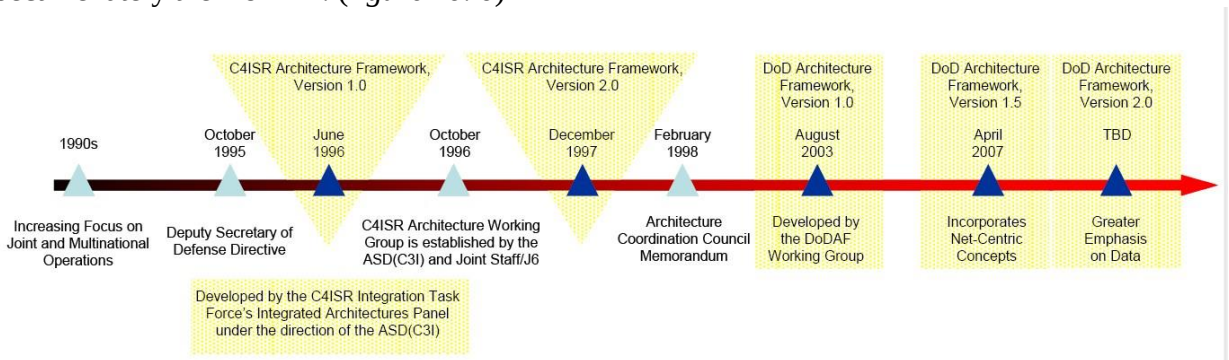

Figure 6 Evolution of the DoDAF since the 1990s. The DoDAF V2.0 was released in May, 2009. (https://www.wikipedia.org)

United States Department of Defence has a long history of systems acquisition where each acquisition program independently developed redundant and incompatible systems. As a solution to these problem, identified in a number of audits, the Department of Defence, prompted establishment of the Global Information Grid, and establishment of the DoD Architecture Framework . As a result, the Network Centric Warefare is the overarching enterprise architecture for communication and information systems within DoD. Also DoD struggled with interoperability issues for various processes and systems as it moved toward integrated task force strategies. The DoDAF provided a necessary basis for comparing architectures and for identifying critical interfaces needed. [10]

In the DoD the net-centric activities are described in detail in the Net-Centric Operations and Warfare Reference Model (NCOW). The NCOW activity Manage Net-Centric Environment consists of the planning, organizing, coordinating, and controlling the establishment, maintenance, and dissolution of all the capabilities of and services provided by the information environment. It comprises the development of the environment's capabilities, the management of its system and network configurations, as well as the conduct of its administration, monitoring, and response activities. (f*igure no. 7*)

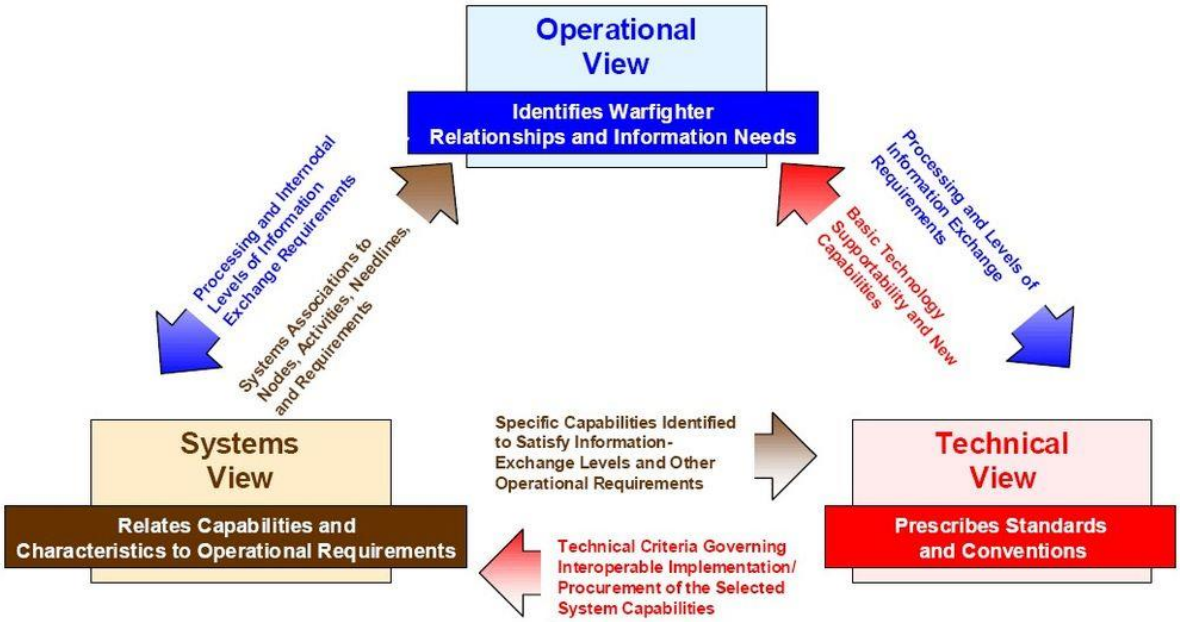

Figure 7 DoD C4ISR Framework (https://www.wikipedia.org)

The DoDAF organizes its views into a set of eight viewpoints, defined in next figure (f*igure no. 8*) . These viewpoints tend to map to abstract classes of stakeholders: executives, business managers, operational personnel, and IT personnel.

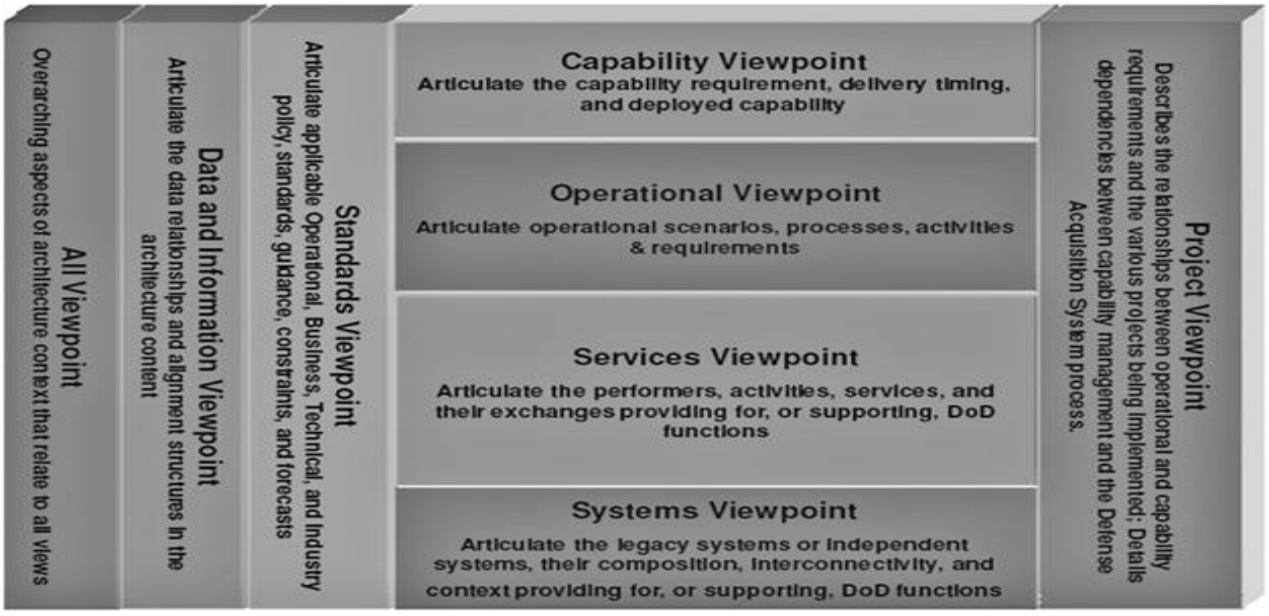

Figure 8 DoDAF viewpoints [5]

Network-centric warfare (NCW) is a new theory or doctrine of war developed primarily by the United States Department of Defence. This emerging theory indicates a radical shift from a platform-centric approach to a network-centric approach to warfare. The US developed the NCW concept in response of the military to the opportunities given by the *informational era*, and it should not be perceived as a simple computer network organized

between different military structures in the battle space. This collaborative communication and information system implies the development of collaborative processes between all military structures present in the theatre of operations, so that they can use the information they need in real time, and also they can provide the necessary information needed to accomplish the mission. So the principle of this revolutionary concept is to allow the participating structures to carry out the mission with full advantage of the information available on the network, for planning and conducting operations.

The basic premise of NCW is that robust networking of geographically dispersed military forces makes it possible to translate informational advantage into warfare advantage. Higher levels of information sharing among the units enhance the extent of "shared situational awareness." In other words, through information sharing, every unit—from infantry units to aircraft to naval vessels to command centres—"sees" the sum of what all other units "see." This shared awareness facilitates self-synchronizing forces, virtual collaboration, and other forms of flexible operations. The value proposition for the military is a significant reduction of combat risks, higher order combat effectiveness, and low-cost operations.

The term network-centric operations (NCO) was originally applied to the field of logistics and supply chain management in business enterprises. The term "value nets" or "value networks" has also been used in this context. However, more recently, NCO has gained a broader interpretation and is often used interchangeably with NCW in the defence and military areas.

The concept of network-centric enterprise (NCE) owes its origin to the concept of business ecosystems and virtual organizations. It involves establishing an "info structure" that connects the different partners in a company's business ecosystem and supports the different value creation processes. As such, the concept of NCE is also closely related to NCO. [9]

The NCW program, as presented in joint Vision 2020, underpins the strategy of transformation of the American Armed Forces. Combatants, weapons and sensors are connected on the basis of the Internet protocol, while ensuring information sharing and *knowledge of the situation*.

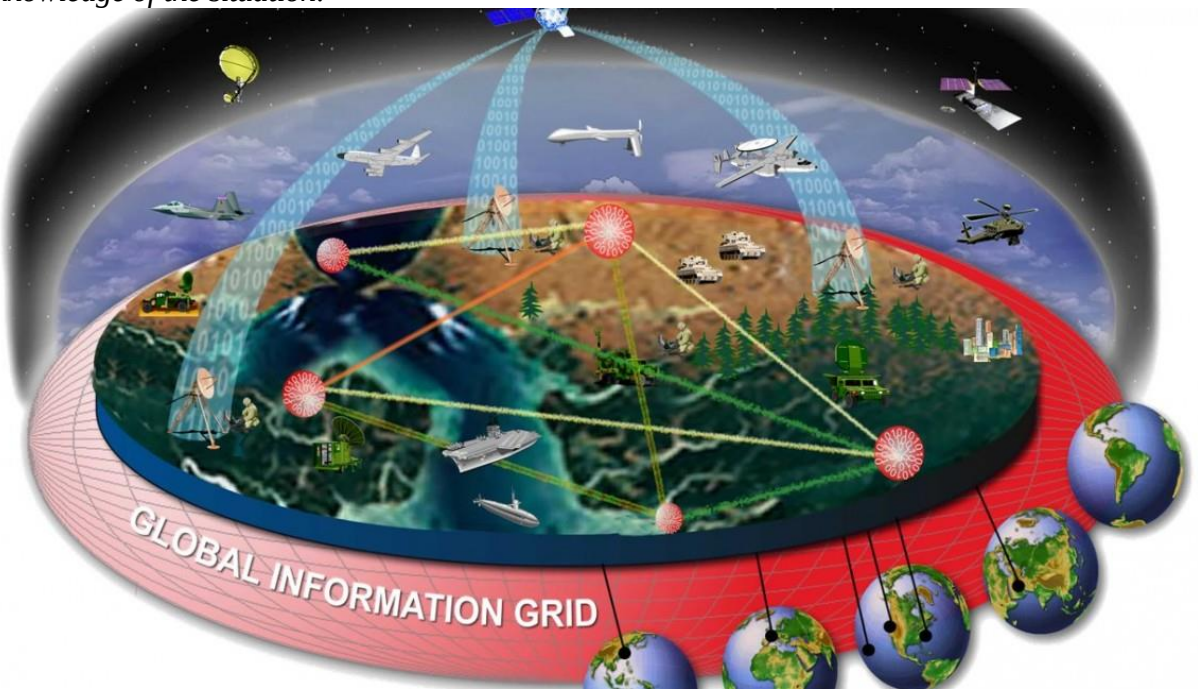

Figure 9 Global Information Grid (GIG) (https://www.wikipedia.org)

The GIG's networks (*figure no. 9*) span a wide spectrum of DoD agencies. Many of these networks are under the jurisdiction of the Defence Information Systems Agency (DISA). Two of the networks maintained by DISA are NIPRNet (Non-secure Internet Protocol Router Network) and SIPRNet (Secure Internet Protocol Router Network). SIPRNet, NIPRNet, the Joint Worldwide Intelligence Communications System (JWICS), and several other secure, acronym-heavy networks make up the DISA's Defence Information Systems Network (DISN). The GIG connects DISN with army network LandWarNet and with all the other networked systems that the military operates—satellites, radios, drone. The GIG is network-centric warfare made manifest: a protocol that allows for each constituent dataset, weapon, or communications tool to be used as building blocks in defence systems greater than the sum of their parts.

6. Collaborative communication and information system used in modern theatres of operations by the NATO

Since the beginning of the concept of NCW, at NATO level, there has been a question of the implementation and development of this concept in order to allow the management of the operations of the Network Enabled Capabilities (NEC)-based alliance, the substantiation document being developed in 2004. Its achievement was done in the light of operational requirements for the transformation of NATO forces and the study of complex scenarios with the engaging of the NRF.

The development of the *NATO Network Enabled Capabilities* (NNEC) concept – was based on the principles of the *Network Centric Warfare* (NCW) and their inclusion in NATO's operating concepts. The purpose of using these principles was to establish clear links between new NATO operations, the vision of strategic commanders to lead these operations and the types of communication an information system capabilities needed for their support.

NATO's Architecture Framework (NAF) is the means by which interoperable systems are obtained through a single representation, a common data model and a common mechanism that allows the models to be changed. NAF facilitates the development of new military capabilities by: identifying capabilities deficits and better integration of existing capabilities; promoting interoperability within NATO; ensuring increased confidence that the requirements of the CIS services users are satisfied; reduce the risk of delays in running programmes with equipment.

The NAF supports capturing the vision of the enterprise in all its dimensions and complexity of system of-interest. The NAF architectures developed will be an important contribution to ensure that the stakeholders of an enterprise are focused on the same goals; development of operational capabilities and the transformational process to reach the objectives of any organization. For illustration, in the defence domain the NATO *Federated Mission Networking* (FMN) is an example of what NAF architectures wil support.

NNEC, as a system federation, aims at a service-oriented approach to provide capabilities. In order to cope with all the requirements, a common framework is needed to ensure consistency and relationships clearly defined between the elements of architecture. Because architecture is an essential part of the strategic framework, NAF is the tool of NATO and member states for the development and implementation of the NNEC and Federated Mission Networking (FMN) vision.

FMN is the key element of the *Connected Forces Initiative* (CFI) concept, helping allied and partner forces better communicate, train and act together.

The FMN concept enables a rapid initiation of mission networks through the federalization of NATO's capabilities and mission partners, thereby increasing interoperability and information sharing.

FMN is a conceptually regulated framework, consisting of people, processes and technologies that plan, establish, use and prepare mission networks in support of federated operations in the theatre of operations. This capability is achieved in order to support the command-control and decision-making processes in future operations by improving the exchange of information. This conceptual framework provides the agility, flexibility and scalability necessary to manage the emerging requirements of any mission environment in future NATO operations. FMN is based on principles that include cost effectiveness and maximum reuse of existing standards and capabilities.

FMN consists of three elements, shown in *figure no. 10*, thus: Governance, **Framework** and Mission Networks.

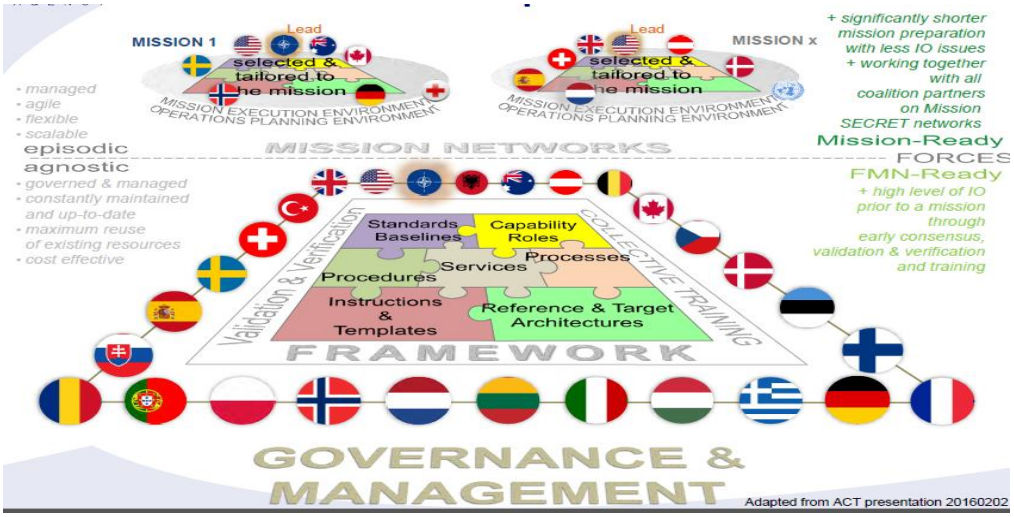

Figure 10 FMN elements (https://www.afcea.de)

Four gradual levels of capability are defined as options for participation in the evolution of FMN in general and for participation in mission networks in particular:

1. **Mission Network Element (MNE)** - contains a network and information infrastructure and services needed for the auto support, including sufficient services essential to accomplish the mission.
2. **Mission Network Extension (MNX)** - contains a network and information infrastructure and services needed for the auto support, but it may not include sufficient services essential to accomplish the mission.
3. **Hosted User (HU) -** is a participant in the Mission network that is unable to provide network and information infrastructure and the services necessary for the Auto support.
4. **Other participants**-participants who do not fall within the situations described above and are not part of the network and are not subject to the framework requirements of FMN.

The ability to share information is an essential factor for the success of military operations. NATO and national collaborative communication and information systems in the theatre of operations must ensure the necessary means of exchanging information on any mission. The basic resources for all information are represented by data, which following a correct interpretation is transformed into information. As the value and cost of data increases, this resource becomes critical. [11]

7. Initiative of implementation of the global, unclassified, collaborative communication and information system.

Based on the challenges associated with conducting coalition and multinational operations, a new multinational initiative that focuses on collaboratively developing and accessing concepts and capabilities, named Multinational Capability Development Campaign (MCDC) appeared. It identifies and evaluates potential solutions to coalition and multinational capability gaps and contributes to multinational capability development. MCDC is focused on developing concepts and theoretical capabilities for joint, multinational and coalition operations to meet present and future operational needs of the US and coalition partners.

The Federated Mission Networking (FMN)/Mission Partner Environment (MPE) Civilian-Military (FMCM) Information Sharing will provide FMN/MPE developers the requirements for CIV-MIL information sharing in consultation with major humanitarian organizations. A new concept of operations and guidebook to support doctrine, tactics, techniques, and procedures, and education development to utilize the spiral development capability will be provided by FMCM to the Multinational Force Commanders and staff.

The aim of this project is to produce for the FMN community validated requirements and standards for CIV-MIL information sharing. Also FMCM will provide an overarching operational concept, implementation guidebook and mission thread architectures outlining key information exchange requirements between the Force Commander and primary humanitarian organizations and government agencies. Products will be nation and region agnostic providing a common principles, lexicon, capability, definitions, standards, best practices and processes, adaptable by all nation affiliated to the community. (*figure no. 11*)

Figure 11 MCDC Force Development Community.(https://slideplayer.com)

FMCM will support and enable planning and execution in a FMN/MPE framework for the timely establishment of effective information sharing, collaboration, cooperation, and coordination with non-military entities across the Civilian- Military operations, including support of sudden onset disasters.

Mission Partner Environment (MPE) is an operating environment that reflects US DoD desire to be an FMN Affiliate and enables Command and Control (C2) for operational support planning and execution on a network infrastructure at a single security level with a common language.

All Partner Access Network (APAN) is an unclassified information sharing and collaboration enterprise supported by the United States Department of Defense (DoD). In APAN network, authorized users can work and collaborate, using specific tools, to leverage information to effectively plan, train and respond to meet their requirements and mission objectives. Individuals and organizations who do not have access to traditional DOD systems and networks can participate in information sharing and collaborative events because these tools are available over the open Internet so.

The FMN framework is based on a structure supporting the varied capabilities of military participants. This includes information sharing with participants not part of the FMN network. Those entities/organizations not directly linked to the FMN network are referred to as Option Z entities in FMN documents. Option Z includes, among others, entities other than Mission Partners who, while not part of the FMN federation, might have information connectivity and associated information sharing capabilities and needs, respectively, with the FMN participants. Examples of Option Z would include UN organizations, an affected state government to include regional disaster coordinators, other responding military forces not part of the FMN framework, non-UN associated humanitarian organizations, and local social development organizations. One example of integration of FMN and MPE is presented in *figure no. 12*.

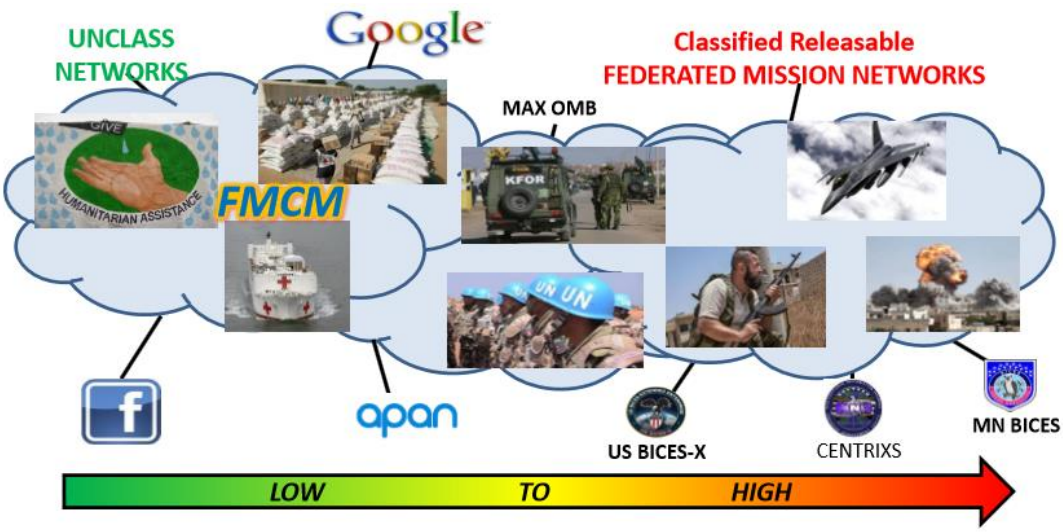

Figure 12 Example of integration of FMN and MPE (https://c2coe.org)

Next figure (*figure no.13*) depicts an information sharing network based on agreed standards and specific joining instructions where mixed capabilities of mission partner military forces are connected under FMN architecture. The concentric rings represent the interconnecting military networks that support the FMN information sharing environment. The FMN architecture share information with non-FMN entities, named Option Z, who operate independently of the FMN structure. In the right hand corner of the figure are represented Non-FMN entities that can be any organization not participating in the FMN architecture.

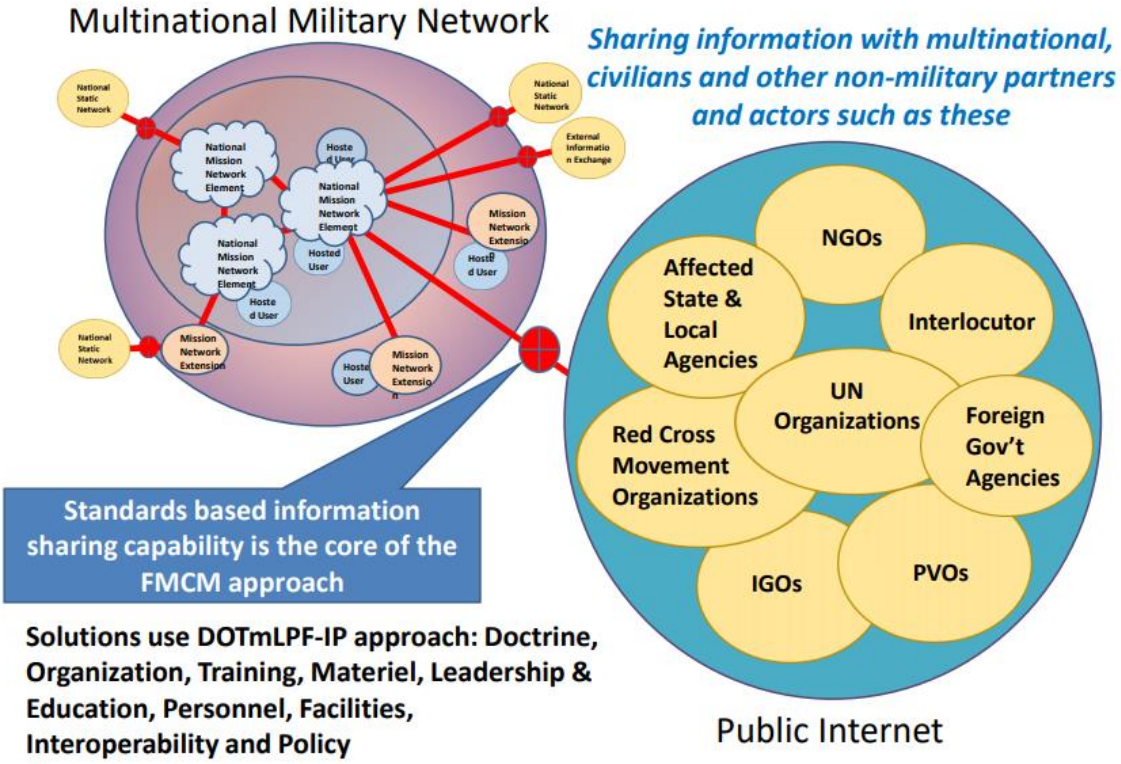

Figure 13 - The mixed capabilities connected in an information sharing network (https://c2coe.org)

The FMN CIV-MIL information sharing concept addresses the new approach of military forces working as a unified information environment serving as a whole-of-effort response to a crisis. FMCM proposed that Mission Thread Package from NATO Architecture Framework (NAF v4) consists of: NAV-1 Overview and summary; NAV-2 Integrated dictionary; NCV-1 Capability vision; NOV-1 Operational concept; NOV-2 Operational nodes; NOV-3 Information requirements; NOV-4 Key organizations; NOV-5 Activity model; NOV-6C Event sequence. [11]

8. Conclusions

Detailing this theme allows us to highlight at least the following ***conclusions***:

- modernisation of communications and information systems is a complex and continuous process, constituting an essential condition for ensuring collaborative work within the entire spectrum of actions specific to the theatre of modern operations;
- in the modern theatres of operations information and informational flow become the main nervous centres, and the decision is increasingly influenced by the new strategy of knowledge;
- in order to achieve a collaborative communication and information system, based on the model of the Federated Mission Networking environment, NATO and the member states of the alliance must be permanently prepared for a gradual increase in bandwidth requirements, which is necessary to achieve the objectives of resilience and redundancy;
- in the collaborative, multinational, inter institutional and inter organisational environment of the modern theatres of operations, ensuring information security will be an essential requirement in the implementation of the Network Federation;

- Informational security involves the implementation of a mission network area based on a common infrastructure, accessible throughout the theatres of operations, allowing the management of classified information throughout the operational area and support for interaction with non-military entities, increasingly present in an effect-based approach;
- an essential requirement is to find informational interface solutions that can ensure the protection, integrity, availability and confidentiality of data based on dynamic principles of access, modification and writing;
- it is also necessary to implement secure collaboration solutions and mechanisms, as well as security policies of appropriate information;
- participation in missions in modern theatres of operations in a FMN/FMCM context requires as a premise in the process of preparing missions to achieve and train collaborative national command and control capabilities, using the same scenarios, the same lessons identified and learned during participation in operations or in collaborative work test exercises;
- in order to achieve an effective connection between the operational and technological environment in the modern theatres of operations, close collaboration is needed between the people responsible for designing, making and using of collaborative communications and information systems, and this can only be done using the architectural framework concept.

References:

[1] Dragomirescu Valentin, *Analysis of searching operations in modern military conflicts*, publicat în „*Conferința Științifică Internațională Strategii XXI – Tehnologii – Aplicații Militare, Simulare și Resurse", Facultatea de comandă și stat major, Universitatea Națională de Apărare „Carol I"*, Volumul 1, București, 2012
[2] Iulian Martin, Raționament si argumentare în planificarea operațiilor, Editura Universității de Apărare „Carol I", București, 2015
[3] Bălăceanu Ion, Dragomirescu Valentin, Martin Iulian, *Interacțiunea strategiilor în conflictele armate moderne*, volumul I, Editura Universității Naționale de Apărare „Carol I", București, 2010
[4] Bălăceanu Ion, *Revoluția tehnologică contemporană și impactul ei asupra potențialului militar*, Editura AISM, București, 2001
[5] Ion Călin, Deficiențe în activitatea de analiză a informațiilor, Editura Universității de Apărare „Carol I", București, 2015
[6] Sorin Topor, Ion Călin, Costinel Nițu, Draga-Nicola Crăcin, Despre informații și sisteme informatice militare, Editura BREN, BucureȘti, 2008
[7] Markus Walker , Stephan Roth , Jesko G. Lamm , Tim Weilkiens, *Model-Based System Architecture*, John Wiley & Sons, 2015, 243-265
[8] Li Da Xu, *Enterprise Integration and Information Architecture*, CRC Press, 2014, 373-411
[9] Andreas Tolk , Larry B. Rainey, *Modeling and Simulation Support for System of Systems Engineering Applications*, John Wiley & Sons, 2015, 145-187
[10] George F. Elmasry, *Tactical wireless communications and networks: design concepts and challenges*, John Wiley & Sons, 2012
[11] Authors, *Certified Enterprise Architect All-in-One Exam Guide*, McGraw-Hill Education, 2018