# DOCTRINAL CONVERGENCES AND DIVERGENCES IN NATO, USA AND EU STRATEGIC ARCHITECTURES AND THE IMPACT ON THE FUTURE OF DEFENSE

***Brigadier-general (ret) Professor Gheorghe BOARU, Ph.D****
***(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania, email: secretariat@aosr.ro)***

***Abstract****: This study analyzes the transformations of the security environment generated by technological convergence and the emergence of new operational paradigms. It is argued that the integration of emerging technologies into extended C4ISR architectures leads to the redefinition of the decision-making cycle and the emergence of decision-making superiority as a determinant of military power.*

*The paper concludes that the future of defense will be defined by the ability of states and organizations to integrate technological convergence into a coherent security ecosystem, oriented towards decisional superiority, societal resilience and cognitive control, thus configuring a new strategic paradigm in which knowledge becomes the main resource of power.*

***Keywords****: emerging technologies, multi-domain operations, doctrinal correlation, decision cycle, cognitive domain.*

**DOI 10.56082/annalsarscimilit.2026.2.93**

## INTRODUCTION

The 21st century is characterized by an unprecedented acceleration of technological progress, which is profoundly influencing the nature of armed conflicts and the architecture of global security. Digital transformation, the development of artificial intelligence, the emergence of quantum technologies and the expansion of cyberspace are driving a paradigm shift: from military superiority based on force to superiority based on information and knowledge.[1].

This evolution leads to the expansion of the battlefield into non-traditional domains, especially in the information and cognitive space. In this context, state and non-state actors adapt their strategies to exploit the vulnerabilities of complex interconnected systems.[2].

Starting from the concepts developed within NATO regarding **Multi-Domain Operations (MDO)** and the emergence of **cognitive warfare**, a structural transformation can be observed in the way

---

* Entitled member of the Academy of Romanian Scientists, entitled member of the Academy of National Security Sciences, email: boarugheorghe@yahoo.com.

[1] Alvin Toffler, *War and Anti-War,* New York: Little, Brown, 1993, pp. 35–40.

[2] Joseph S. Nye, *The Future of Power,* New York: PublicAffairs, 2011, pp. 113–120.

contemporary military operations are conceived and executed. MDO represents a major doctrinal evolution, defined as the integrated orchestration of military and non-military actions in all domains – land, air, maritime, cyber, space and information – with the aim of generating convergent effects "at the speed of relevance".

This approach implies a fundamental paradigm shift: from sequential operations, focused on distinct domains, to **simultaneous, interconnected and synchronized operations**, in which advantage is no longer determined solely by the mass of force, but by the ability to integrate information and rapidly generate strategic effects. In this context, digital transformation becomes an essential catalyst, with NATO evolving towards a **data-centric model**, capable of collecting, sharing and exploiting data from all operational domains.

In parallel, the development of the concept of **cognitive warfare** extends the battlefield to the human dimension, where perceptions, behaviors and decision-making processes become direct targets of strategic actions. Cognitive warfare is defined as the set of activities aimed at influencing or degrading individual and collective cognition in order to obtain operational advantage. In this logic, "the human mind becomes the battlefield", and operational success depends on the ability to shape perceived reality, not just physical reality.

## 1. TECHNOLOGICAL CONVERGENCE AND IMPACT ON THE FUTURE OF DEFENSE

Technological convergence represents the integration and synergistic interaction of multiple technological fields, especially nano-, bio-, info- and cogno-technologies (NBIC)[3]. This convergence generates multiplier effects, accelerating innovation and radically transforming military capabilities.

### 1.1. Emerging technologies:

- artificial intelligence and machine learning;
- quantum computing;
- biotechnology;
- autonomous systems;
- space technologies.

### 1.2. Strategic effects:

- increasing operational speed;
- decision automation;
- reducing dependence on the human factor;

[3] Mihail C. Roco and William Sims Bainbridge, *Converging Technologies for Improving Human Performance,* NSF, 2002, pp. 13–25.

• emergence of systemic vulnerabilities [4].

**2. MULTI-DOMAINE OPERATIONS**

**Doctrinal correlation:** NATO Allied Command Transformation – NATO Warfighting Capstone Concept (NWCC) (2023); NATO – Strategic Concept (2022).

Multi-domain operations represent a major doctrinal evolution, characterized by the integration of actions in all domains of operation: land, air, maritime, cyber, space and information[5].

**2.1. Main features:**

• real-time synchronization;

• interoperability;

• integration of multiple actors.

**2.2. Implications:**

• increased complexity;

• need for information superiority [6].

**3. EXTENDED C4ISR AND DIGITAL TRANSFORMATION**

**Doctrinal correlation:** U.S. Department of Defense – CJADC2 Implementation Guidance (2024); DoD – Data, Analytics, and AI Adoption Strategy (2023); NATO – Data Exploitation Framework Policy (2023).

C4ISR architectures are evolving towards extended models that integrate artificial intelligence and advanced data processing technologies [7].

**3.1. Components:**

• command & control;

• communications;

• computers;

• intelligence;

• surveillance;

• reconnaissance.

**3.2. Extensions:**

• AI and advanced analytics;

---

[4] Klaus Schwab, *The Fourth Industrial Revolution,* Geneva: World Economic Forum, 2016, pp. 7–15.

[5] NATO Allied Command Transformation, *Multi-Domain Operations Concept,* 2023, pp. 10-18; NATO Allied Command Transformation, *Multi-Domain Operations Concept,* 2020, pp. 5-9.

[6] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare,* CCRP, 1999, pp. 88–95.

[7] DoD – *Data, Analytics, and AI Adoption Strategy,* 2023, pp. 7–15; David S. Alberts and Richard E. Hayes, *Power to the Edge,* CCRP, 2003, pp. 45–60.

- cloud and edge computing;
- quantum technologies [8].

**4. REDEFINING THE DECISION-MAKING CYCLE**

**Doctrinal correlation:** RAND Corporation – Accelerating Decision Advantage in Multi-Domain Operations (2022); NATO – Emerging and Disruptive Technologies Strategy Update (2024).

The OODA (Observe–Orient–Decide–Act) model is redefined in the context of technological convergence[9].

**4.1. Transformations:**

- automation of the observation stage;
- augmentation of the orientation stage;
- acceleration of the decision.

**4.2. Augmented OODA:**

- integration of AI;
- distributed decision;
- interconnected loop [10].

**5. COGNITIVE DOMAIN**

**Doctrinal correlation:** NATO – Countering Cognitive Warfare (2021, operationally used in 2022–2024); NATO Innovation Hub – Cognitive Warfare.

The cognitive domain becomes a central space of modern conflict[11].

**5.1. Characteristics:**

- influencing perceptions;
- information manipulation;
- psychological operations.

**5.2. Impact:**

- degrading the adversary's decision-making process;
- creating uncertainty [12].

[8] Elsa B. Kania and John K. Costello, *Quantum Hegemony?,* CSIS, 2017, pp. 12–18.

[9] RAND Corporation – *Accelerating Decision Advantage in Multi-Domain Operations,* 2022, pp. 22–30; John Boyd, "A Discourse on Winning and Losing", unpublished briefing, 1987, pp. 3–10.

[10] Paul Scharre, *Army of None,* New York: W.W. Norton, 2018, pp. 121–135.

[11] Bernard Claverie and François du Cluzel, *Cognitive Warfare,* NATO Innovation Hub, 2020, pp. 4–9.

[12] NATO, *Countering Cognitive Warfare*, 2021, pp. 6–12.

**6. STRATEGIC ADVANTAGE: DECISION-MAKING SUPERIORITY**

**Doctrinal correlation:** U.S. National Defense Strategy (2022); RAND (2022); CSIS – AI and the Future of Warfare (2024).

Decisional superiority is the ability to make decisions faster and more effectively than the adversary[13].

**6.1. Driving factors:**

- data access;
- processing capacity;
- information integration.

**6.2. Results:**

- higher operational tempo;
- convergent effects [14].

**7. VULNERABILITIES AND RISKS**

- technology addiction;
- cyber attacks;
- ethical issues [15].

**8. STRATEGIC IMPLICATIONS**

**Doctrinal correlation:** European Union – Strategic Compass (2022); UK MoD – Defence Command Paper Refresh (2023); NATO Strategic Concept (2022).

- doctrinal adaptation;
- investment in research;
- education and resilience[16];
- doctrinal adaptation;
- investment in research;
- education and resilience [17].

Following the analysis of the main concepts presented above, I present a **comparative synoptic table (NATO vs USA vs EU)** for the key concepts: **MDO, C4ISR/CJADC2, Cognitive Warfare, Decision Superiority.**

[13] DoD – *Data, Analytics, and AI Adoption Strategy,* 2022, pp. 5–12; Martin C. Libicki, *Conquest in Cyberspace,* Cambridge University Press, 2007, pp. 45–52.

[14] Frank Hoffman, "Hybrid Warfare," *Joint Force Quarterly,* 2007, pp. 14–20.

[15] Luciano Floridi et al., "AI4People—An Ethical Framework for a Good AI Society," *Minds and Machines,*2018, pp. 689–707.

[16] European Union – *Strategic Compass,* 2022, pp. 8–20.

[17] RAND Corporation, *The Future of Warfare in 2030,* 2019, pp. 22–30.

**Comparative synopsis table (NATO vs USA vs EU)[18]**

| Concept | NATO | USA | European Union (EU) |
|---|---|---|---|
| **MDO (Multi-Domain Operations)** | Conceptually adopted within the NATO Warfighting Capstone Concept (NWCC) and adapted through MDO/All-Domain Operations alignment between land-sea-air-space-cyber domains. Emphasis on allied interoperability and multi-domain integration in collective operations. | Central doctrinal concept US Army / Joint Force. MDO = integration of simultaneous effects in all domains (land, air, sea, cyber, space, cognitive). Offensive vision: "penetrate, dis-integrate, exploit, re-compete". | It does not have a unified MDO doctrine. The approach is fragmented: PESCO + Strategic Compass promotes the integration of multi-domain capabilities, but without a unified operational concept equivalent to NATO/US. |
| **C4ISR / CJADC2** | NATO is developing **Federated Mission Networking (FMN)** and the **NATO Digital Transformation / C2 Integration concept**. CJADC2 is tailored as allied interoperability, not as a single system. | The US is directly developing **CJADC2 (Combined Joint All-Domain Command and Control)** – a unified network of sensors–decision makers–effectors. Integrating AI, cloud, edge computing for real-time decision making. | EU is developing **CDI (Common Defence Intelligence) and EU C2/MPCC** initiatives, but without fully integrated CJADC2 architecture. Emphasis on digital sovereignty and limited interoperability. |
| **Cognitive Warfare** | NATO officially recognizes the cognitive domain as part of the hybrid competition (e.g. NATO Innovation Hub). Emphasis on the "human domain", informational influence and societal resilience. | The USA integrates into the concept of **Information Advantage / Cognitive Domain Operations (US Army, USMC)**. Includes PSYOP, MISO, AI-driven influence operations. | The EU approaches through **the strategy to combat disinformation (EEAS StratCom) and the Digital Services Act.** Defensive-normative focus (information resilience). |
| **Decision Superiority** | NATO defines it as a result of **information superiority and alliance interoperability.** It | Central concept in the US **Joint Force doctrine: "decision advantage /** | The EU pursues "**strategic autonomy in decision-making**", but is limited by the intergovernmental |

[18] Own conceptual synthesis based on NATO (NWCC), US (CJADC2) and EU (Strategic Compass) doctrinal documents.

| | | | |
|---|---|---|---|
| | depends on allied consensus and data sharing between states. | **decision dominance**" – accelerating the OODA cycle through AI, distributed sensors and decisional autonomy. | process. Decision-making is slower, based on political consensus. |

**As a comparative essence, the following synthesis is evident:**

• **The US** is a **conceptual and technological leader:** it dominates the integration of CJADC2 + MDO + cognitive operations into a unified ecosystem**;**

• **NATO** has a **collective interoperability architecture,** not a single system; role as a "framework integrator";

• **The EU** is an **emerging actor in the field of defense,** with a focus on regulation, resilience and limited strategic autonomy, but without full operational integration**.**

The comparative analysis reveals that, despite institutional and doctrinal differences, NATO, the US and the EU are evolving towards a common model of warfare based on data integration, cognitive dominance and decisional superiority. **The table** summarizes this convergence, while highlighting the differences in emphasis: the US privileges the technological dimension, NATO the interoperability dimension, and the EU the political-strategic dimension.

This complementarity can form the basis of an integrated Euro-Atlantic security architecture[19].

## 9. CONCLUSIONS

This study analyzes the profound transformations of the security environment in the 21st century, generated by technological convergence and the emergence of new operational and doctrinal paradigms. In the context of the acceleration of the development of emerging technologies – artificial intelligence, quantum computing, biotechnologies and autonomous systems – a strategic mutation is highlighted from the traditional paradigm of military superiority based on kinetic force towards a model centered on **informational and cognitive dominance**.

[19] European Union, *A Strategic Compass for Security and Defence*, pp. 23–30.

Starting from the concepts developed within NATO regarding multi-domain operations and cognitive warfare, the paper argues that the integration of technologies in advanced architectures of the extended C4ISR type (C4ISR+AI+Quantum) leads to the redefinition of the decision-making cycle and its significant compression, in the logic of the OODA Loop model. Thus, the strategic advantage is transferred to actors capable of efficiently managing massive volumes of data and transforming information into relevant operational knowledge in real time.

The study also explores the emergence of the cognitive domain as a new space of confrontation, where perceptions, trust and social cohesion become direct targets of hostile actions. In this regard, the role of information warfare, psychological operations and artificial intelligence-based technologies in shaping individual and collective behavior is highlighted.

Methodologically, the research uses conceptual and comparative analysis of specialized literature, including relevant contributions from think tanks such as RAND Corporation and CSIS, as well as recent case studies that illustrate the practical application of technological convergence in contemporary conflicts.

We can conclude that the future of defense will be defined by the ability to integrate technologies and transform information into operational knowledge. Decisional superiority becomes the central element of military power.

## BIBLIOGRAPHY

ALBERTS D. S., GARSTKA J., STEIN F., *Network Centric Warfare.* CCRP, 1999;

ALBERTS D. S., HAYES R., *Power to the Edge,* CCRP, 2003;

BOYD J., *"A Discourse on Winning and Losing"*, Unpublished briefing, 1987;

CLAVERIE B., du Cluzel F., *Cognitive Warfare,* NATO Innovation Hub, 2020;

FLORIDI L. et al., "AI4People—An Ethical Framework for a Good AI Society," *Mind and Machines* (2018);

HOFFMAN F., "Hybrid Warfare," *Joint Force Quarterly* (2007);

KANIA E. B., COSTELLO J.K., *Quantum Hegemony?* CSIS, 2017;

LIBICKI M. C., *Conquest in Cyberspace,* Cambridge University Press, 2007;

NYE J.S., *The Future of Power,* New York: PublicAffairs, 2011;

ROCO M., BAINBRIDGE W.S., *Converging Technologies for Improvin Human Performance.* NSF, 2002;
SCHARRE P., *Army of None.* New York: W.W. Norton, 2018;
SCHWAB K., *The Fourth Industrial Revolution.* Geneva: World Economic Forum, 2016;
TOFFLER A., *War and Anti-War*, New York: Little, Brown, 1993;
RAND Corporation, *The Future of Warfare in 2030* (2019);
NATO Allied Command Transformation, *Multi-Domain Operations Concept* (2020);
NATO Allied Command Transformation, *Multi-Domain Operations Concept* (2023);
NATO, *Countering Cognitive Warfare* (2021);