NEW SECURITY PARADIGMS AND THEIR IMPACT ON INFORMATION SYSTEMS

Colonel (ret) Professor Gruia TIMOFTE, Ph.D*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania, email: secretariat@aosr.ro)

Abstract: *This paper presents the main aspects regarding the technological convergence of information systems from various fields in the security environment and has as its main objective the satisfaction of all technical, functional and operational requirements of all elements in the modern battlespace. Also, the in-depth study of these systems highlights the need to train all categories of personnel for their efficient use and obtaining superior operational performances in conditions of effective cooperation and interoperability.*

Keywords: *paradigm, security, convergence, integration, data-centric, computing.*

DOI 10.56082/annalsarscimilit.2026.2.69

1. INTRODUCTION

The fourth industrial revolution describes the rapid technological advancements of the 21st century. Part of this phase of industrial change is the merging of advanced technologies such as artificial intelligence (AI), gene editing with advanced robotics, which blur the boundaries between the physical, digital and biological worlds. The integration of modern intelligent technology, large-scale machine-to-machine communication and the Internet of Things (IoT) is leading to increased automation, improved communication and self-monitoring, the use of intelligent machines that can analyze and diagnose various problems without the need for human intervention.[1]

Technological convergence is the tendency for technologies that were initially unrelated to each other to become closely integrated and even unified as they develop and implement. For example, telephones, television, computers, and social media platforms began as separate, largely unrelated technologies, but have since evolved into an interconnected telecommunications, media, and technology industry. Convergence is the deep integration of relevant human knowledge, tools, and activities toward a

* Entitled member of the Academy of Romanian Scientists, Military Sciences Section, phone: 0731684461, email: timmy.gruia@yahoo.com.

[1] McKinsey & Company, *The Industry 4.0, the Fourth Industrial Revolution*, and 4IR, First programmable controller based automation), 2014.

common goal, enabling society to respond to new demands for changing physical or social ecosystems[2].

Integration is a transformation process measured by the degree to which diverse technical environments, such as telephony, data transmission, and information technology infrastructures, are combined into a single platform with a universal network architecture.

Digital convergence is the tendency for diverse digital innovations and environments to become closer together over time. This type of technological convergence creates new opportunities, especially in the field of product realization and development strategies for digital product companies. In this situation, digital convergence encompasses three phenomena:

- previously independent devices are connected through networks and software, significantly improving the functions of the systems;
- previously independent products are converged on the same platform, creating hybrid products;
- companies overcome traditional boundaries for some products, such as hardware and software, in order to offer new ones.

Convergence can also refer to the ability to run the same application on different devices and develop applications for other devices simultaneously, with the same code base[3].

2. NEW SECURITY PARADIGMS IN THE 21ST CENTURY

A security paradigm is the conceptual framework and fundamental approach by which threats are identified, assessed and managed. It is evolving from traditional models, focused on the state and military defense, towards a modern, social, ecological and digital perspective, focused on resilience, cooperation and human security in the face of complex risks, such as climate change or cyber attacks.

New security paradigms in the 21st century have evolved from a focus on state military defense to a multidimensional concept, defined by hybrid, non-state and technological threats. Modern security integrates economic, cyber, social and health dimensions, being influenced by technological convergence and globalization.

The essential characteristics of these new paradigms include [4]:

- the shift from state security to human security: the focus is on protecting the individual and the community, not just borders;

[2] David Messerschmitt, *The Prospects of Computing Communications Convergence,* Munich, Germany, 2007.

[3] Cristian Barna, Valentin Nicula, *Security Paradigms in the 21st Century*, RISR, No. 23, Bucharest, 2020, pp. 122-124.

[4] Gabriel Gabor, *Caracteristici ale paradigmelor de Securitate în secolul XXI*, Bucharest, 2014, pp. 35-37.

- hybrid and non-state threats: non-state actors and cyberattacks, along with disinformation, define new conflicts;

- technological convergence: Artificial intelligence and emerging technologies are reconfiguring defense and intelligence;

- transnational security targets issues such as terrorism, pandemics and climate change that require international cooperation, going beyond classical neorealist approaches.

This transformation involves a redefinition of international relations and security models, moving from a purely military approach to a holistic one, based on information and cybersecurity.

Security in the 21st century has ceased to target only the means of combat and borders, moving from the traditional (military) vision to a multidimensional one.

The main paradigm shifts are [5]:

- Human security: The focus has shifted from protecting the state to protecting the individual. This includes economic, food, personal and health security.

- Broadening the spectrum of analysis: Security now encompasses five essential sectors: **military, political, economic, societal and environmental**. An economic crisis or the collapse of ecosystems are seen as direct threats to stability.

- Asymmetric and hybrid threats: We are no longer talking only about wars between regular armies, but also about terrorism, cyber attacks, disinformation and energy pressures. The border between "peace" and "war" has become very diffuse.

- Cybersecurity: Critical infrastructure (communication routes, electricity, banks, hospitals) is now vulnerable to remote attacks, turning digital code into a weapon as dangerous as a projectile.

- The return of great power competition: While transnational threats (climate change) persist, we are witnessing a return of classic geopolitical rivalries but in a context of total economic interdependence.

- Artificial Intelligence is not just a new technology, but a force multiplier that is redefining the speed and nature of modern conflicts. It functions as a "double-edged sword", offering immense tactical advantages, but also new vulnerabilities.

The main directions of in-depth study are:

a. Cyber war and Security[6]:

b. AI transforms digital security from a reactive process to a predictive and autonomous one. Automatization of attacks:

[5] Cristian Alexandru, *Schimbarea paradigmelor in mediul internațional de securitate*, Intelligence Info No. 3, vol.2, 2023, pp. 72-73, 80-81.

[6] Peter Singer, Allan Friedman, *Cybersecurity and Cyberwar*, Oxford University Press, 2014.

• Attackers are using AI to discover vulnerabilities in seconds, a process that previously took hours.

• Proactive defense: Defensive systems can detect anomalies and respond to incidents in real time, without constant human intervention.

• Autonomous systems: Software agents are emerging that are capable of adapting attack or defense strategies "on the fly," surpassing the responsiveness of human analysts.

c. Perception manipulation and information warfare:

AI has multiplied the creation of fake content, turning disinformation into a threat to democratic stability.

• Deepfakes and voice cloning: These can be used to discredit political leaders or induce social panic.

• Micro-targeting: Algorithms analyze massive data to deliver personalized disinformation messages that exploit the specific fears of certain population groups.

d. Intelligence and strategic analysis:

For intelligence agencies, AI is the solution to the big data challenge of the 21st century.

• Big Data Analytics: Can correlate billions of open-source data points to predict crises or troop movements.

• Early Warning: Predictive models can identify weak signals that signal a terrorist attack or geopolitical crisis before they materialize.

e. Ethical dilemmas and existential risks:

Integrating AI into security raises fundamental questions about human control.

• The "Human-in-the-loop" principle: There is intense debate about whether the decision to use lethal force should ever be left to an algorithm ("black box").

• Autonomous weapons systems: These promise to reduce the risk to one's own soldiers, but increase the risk of accidental escalation of conflicts.

In our country, the emphasis is on ethical use and increasing cyber resilience in the face of these new challenges.

3. TECHNOLOGICAL CONVERGENCE IN THE CONTEXT OF NEW SECURITY PARADIGMS

It represents the fusion of advanced digital technologies, physical security, and analytics capabilities, redefining how threats are detected, prevented, and managed in the 21st century. This integration blurs the boundaries between cyber and physical security, creating unified ecosystems.

Key Technology Convergence Trends (2025-2026)[7]:

Edge AI: Modern cameras and sensors integrate native AI to move from simple motion detection to behavioral understanding (e.g., identifying 'wandering', abandoned objects, crowds, or aggression).

• *Unified Hybrid Systems: Integrating CCTV, access control, and intrusion systems into a single management platform gives operators a holistic view of the security situation.*

• *Predictive Analytics: Modern technologies use data to predict potential threats before they materialize.*

• *IoT and Cybersecurity: The large number of connected devices (IoT) requires robust cybersecurity to prevent them from becoming entry points for attackers.*

The new security paradigms are:

• Technological security: It is becoming a crucial area, with technology dependency meaning that investments in this sector are essential to not be left behind.

• Resilience of critical entities: Convergence requires increased attention to the security of critical infrastructures, AI and data privacy.

• Quantum and human technologies: The convergence elements of these technologies are identified as tools that fundamentally change the paradigm of security and human "improvement".

In our country, challenges include the need for adaptation through retraining and the use of digital technologies, given the importance of information and economic security as a support for military security.

Technological convergence in new security paradigms leads to the disappearance of the boundaries between physical, cyber and governance systems. We are no longer talking about isolated solutions, but about an interconnected ecosystem.

The main pillars of this evolution are the following[8]*:*

a. IoT integration with territorial infrastructure: Security no longer only targets data on servers, but also critical infrastructure (electricity grids, transport). A cyber attack now has immediate physical consequences.

b. Artificial Intelligence and automation: AI is used dually. On the one hand, for proactive anomaly detection (identifying attacks before they occur), and on the other hand, in order to create means and procedures for protection.

c. Cloud native and Zero trust: The transition from the concept of a "secure perimeter" to that of "zero trust", where the user's identity is constantly verified, regardless of location or device.

[7] *** US Congressional Research Service, *The Army' Project Convergence*, Washington, DC, 2022, pp.2-3.

[8] Jeremy Gannon, *Telecom Systems Integration*, University of Phoenix, USA, 2024, pp. 4-5.

d. Big Data and predictive analytics: The ability to process massive volumes of data in real time to correlate seemingly disparate events that, together, indicate a complex security breach.

e. Blockchain for integrity: The use of distributed ledgers to ensure data non-repudiation and secure supply chains.

Main effect:

Security has become a business and national security function, not just an IT department task.

Technological convergence is transforming defense strategies from a reactive and fragmented model to a proactive and unified one. The main changes in companies' defense strategies are aimed at[9]:

a. *Unifying physical and cyber security*

Companies are moving away from managing the two domains separately to eliminate interdependent vulnerabilities.

• Integrated alarm systems: Using IoT sensors and cloud-based access control to create a shared digital-physical shield.

• Cross-functional teams: Creating common command structures between IT and physical security departments to respond to incidents in a coordinated manner.

• Efficiency through synergy: Reducing costs by eliminating redundant investments in equipment that can serve both domains (e.g., AI-enabled security cameras and IT data streams).

b. *From perimeter to zero trust*

The traditional model is considered obsolete in 2026 due to hybrid work and the cloud.

• Continuous verification: The strategy assumes that no user or device (internal or external) is inherently trusted.

• Micro-segmentation: The network is divided into small segments to prevent attackers from moving laterally within the system.

c**.** *AI based defence*

As attackers use AI to automate breach control, companies are adopting autonomous defense strategies.

• Real-time anomaly detection: Machine learning algorithms analyze user behavior to identify subtle attacks before they cause damage.

• Automated response: Automate counter-attack actions to instantly block suspicious IP addresses or isolate compromised accounts.

d. *Supply chain resilience*

Strategies now extend beyond the company itself to suppliers and partners.

[9] Quentin Hodgson, Susan Gates, *Getting the Fundamentals of Cyberspace Force Readiness Right*, Rand Corporation, Santa Monica, USA, 2025.

• Third-party monitoring: Constantly auditing the security posture of software and cloud service providers to prevent springboard attacks.

e. *Compliance-driven strategy*

Security has become a business pillar imposed by increasingly stringent regulations.

• Standardization: Adopting standardized protocols to ensure interoperability of defense systems at the regional and global levels.

4. DEVELOPMENT OF NEW DATA-CENTRIC COMMUNICATIONS AND COMPUTER SYSTEMS

Convergence of new data-centric communications and computing systems[10] represents the fusion of high-performance computing infrastructures, storage technologies and advanced networks, with the aim of efficiently processing very large volumes of data (Big Data) directly at the source or in its proximity. This integration transforms traditional architectures, putting data and its utility at the center of technological development.

The essential elements of the paradigm shift include:

Shift from traditional to modern security: The traditional paradigm, based on realism and border defense, is being replaced by non-traditional approaches that include cyber, economic and ecological security.

• *Socio-ecological security:* Emphasis is placed on transnational threats, such as climate change, biodiversity loss and food/water insecurity, the need for an integrated approach.

• *Data-centric cybersecurity:* New digital paradigms focus on protecting data and users as opposed to old models focused only on the network perimeter.

• *Cooperative European Security* - new approach in Europe, based on cooperation, resilience and strategic security.

• *Human security* - focusing on the well-being of individuals and their safety, not just on state security.

This change is triggered by the complexity of new threats, which can no longer be managed solely through military force, but require an integrated approach and a better understanding of interconnected risks.

The main aspects of the convergence of these systems are[11]:

• *Internet of Things and Edge Computing:* IoT enables the connection of billions of devices, transforming from a connectivity technology into a connectivity paradigm that generates enormous volumes

[10] Mrs. N. Gayathri, *Computer Communications and Networks,* The American College, Mumbai, India, 2021.

[11] Alexandra Zabala-Lopez, Sonia Haiduc*, Data-centric technologies supporting decision-making*, Defence Technology, No. 43, 2024, pp. 226-246.

of data. Convergence with Edge Computing allows this data to be processed locally, reducing latency and bandwidth requirements.

• *Artificial Intelligence and Big Data:* AI is at the heart of digital transformation, analyzing collected data to extract relevant information, with applications in various fields, from e-government to the private sector.

• *Communications and Information Systems (C4ISR):* In critical areas, such as military or security, a fusion between command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems is observed. This ensures rapid processing of information in crisis situations or electronic warfare.

• *Digital Transformation and e-Government:* The implementation of Big Data systems and cybersecurity solutions in public administration and the private sector improves document management and archiving.

• *Resource Management and Quality of Service:* New data-centric systems integrate quality of service control algorithms to efficiently manage IT resources in modern networks. This convergence leads to an information society based on the intensive use of information, decisively influencing economic and social activities.

The convergence of communications and computing systems into a data-centric model represents the transition from traditional networks, where the emphasis was on connecting devices, to an infrastructure where the priority is efficient and secure access to information, regardless of the physical location of the resources.

The main pillars of this convergence are:

a. *Evolution towards Data Distribution Service (DDS)*

Unlike classic client-server models, modern systems use standards that offer a "publish-subscribe" model.

• Decoupling: Communication is decoupled in time and space because applications do not need to know where the other components are located.

• Global Data Space: Creates a shared virtual data space, facilitating interoperability in complex environments such as Industrial IoT.

b. *Cloud-Edge-IoT Integration*

Convergence involves eliminating barriers between local and centralized processing:

• Edge Computing: Data processing moves closer to the source (sensors, mobile devices) to reduce latency.

• Coherent Infrastructures: At the government and industrial level, the aim is to create integrated digital infrastructures that ensure the flow of data between different institutions or departments.

c. *The Impact of Big Data and AI Technologies*

Data-centric systems transport data and analyze it in real time.

• Operational Efficiency: The use of Big Data systems allows for increased efficiency of public and private services through predictive analysis.

• Intelligent Maintenance: The integration of AI allows for real-time monitoring of complex resources.

d. *Security in the New Model*

In a data-centric system, security moves from the central level to the component elements.

Zero Trust: Access is constantly verified, regardless of whether the request comes from inside or outside the network.

• European Standards: Digital transformation strategies, such as those implemented in some urban centers, emphasize the cyber resilience of these converged systems.

In the military field, the transition to data-centric systems marks the shift from "Network-Centric Warfare", where the emphasis was on the physical connection between platforms, to an architecture in which data is treated as a strategic asset independent of the network or application that generated it.

This evolution is essential for modern concepts such as JADC2 (Joint All-Domain Command and Control), used by NATO forces to ensure "decisional advantage" over adversaries.

Characteristics of Data-Centric Military Systems[12]:

Modern systems must comply with the principles established by the US Department of Defense and adopted as a reference within NATO, which specify the requirements imposed on data.

Essential Components and Technologies (2024-2026):

1. *Internet of Military Things (IoMT)*: A network of sensors worn by soldiers, autonomous vehicles and equipment that communicate in real time.

2. *Artificial Intelligence and Big Data*: Algorithms that process huge volumes of information (satellite images, intercepts) to provide necessary elements of action and predictive maintenance.

3. *Digital Twins*: The use of virtual replicas of the battlefield to test tactical scenarios without human risks.

4. *Edge Computing & Cloud Hybrid*: Processing data directly on the battlefield to reduce latency, followed by synchronization with strategic data centers.

5. *Zero Trust Security*: Every request for data access is rigorously verified, eliminating the idea of an implicit "secure internal network".

*The Operational Advantages are***:**

[12] Teamraft, *Data Platforms for a Data-Centric Force*, Whitepaper, Reston, USA, 2026, p. 30.

• *Elimination of information silos:* Data from artillery, intelligence and logistics are integrated into a common operational picture.

• *Speed of reaction:* Shortening the OODA (Observe-Orient-Decision-Action) cycle, allowing commanders to make decisions faster than the adversary.

• *Interoperability between Allies:* Allows multinational forces (e.g. within NATO) to collaborate effectively by using specific standards.

5. CONCLUSIONS

The article addresses some particularly important issues for command and communications structures in the process of transitioning to the new regulations regarding the implementation of the data-centric concept in which the primary elements are 'data'. Thus, the collection, processing and presentation of data is carried out in cloud computing centers and stored in databases. The beneficiaries of this data have data access rights (symbols of 1 – signal with current, 0 signal null), depending on the role performed within the staff or unit, using specific applications.

The transition from classic information systems to data systems represents efforts to equip with technical means and specialized software products, training of all personnel with access procedures, use, security, resilience, interoperability, etc.

The preparation process for the new data-centric system must begin in educational institutions, military units, national training improvement centers and NATO and EU centers, etc.

BIBLIOGRAPHY

ALEXANDRU C., *Schimbarea paradigmelor in mediul internațional de securitate*, Intelligence Info No.3, vol. 2, 2023;

BARNA C., NICULA V., *Security Paradigms in the 21st Century,* RISR, No. 23, Bucharest, 2020;

GABOR G.*, Caracteristici ale paradigmelor de Securitate în secolul XXI*, Bucharest, 2014;

GANNON J., *Telecom Systems Integration*, University of Phoenix, USA, 2024;

GAYATHRI N., *Computer Communications and Networks,* The American College, Mumbai, India, 2021;

HODGSON Q., GATES S., *Getting the Fundamentals of Cyberspace Force Readiness Right*, Rand Corporation, Santa Monica, USA, 2025;

MESSERSCHMITT D., *The Prospects of Computing Communications Convergence*, Munich, Germany, 2007;
SINGER P., FRIEDMAN A., *Cybersecurity and Cyberwar*, Oxford University Press, 2014;
ZABALA-LOPEZ A., HAIDUC S., *Data-centric technologies supporting decision-making,* Defence Technology, No. 43, 2024;
Teamraft, *Data Platforms for a Data-Centric Force*, Whitepaper, Reston, USA, 2026;
McKinsey & Company*, The Industry 4.0, the Fourth Industrial Revolution, and 4IR*, First programmable controller (based automation), 2014;
*** US Congressional Research Service, *The Army' Project Convergence,* Washington, DC, 2022;