

Cyber-Physical Intelligence in Defense Applications

Deheina Reguia¹

¹ Badji Mokhtar Annaba University, reguia.deheina@univ-annaba.dz

Received: 12/07/2026

Accepted: 23/09/2026

Published: 15/10/2026

Abstract:

The military application of cyber-physical systems (CPS) has evolved beyond conventional automation, fundamentally reshaping modern operational doctrines. By integrating autonomous decision-making with seamless operational coordination, these systems have become indispensable to future warfare.

This study examines CPS through a dual lens: a conceptual review of theoretical foundations and a practical analysis of their deployment across digital and physical domains. Utilizing a descriptive-analytical approach, the research highlights the contemporary integration of technology within military frameworks.

Keywords: military domain ; artificial intelligence ; cybersecurity; Internet of Things ; intelligent military equipment.

Corresponding author: Reguia Deheina, reguia.deheina@univ-annaba.dz

INTRODUCTION

The nature of warfare in the current era has undergone a major transformation with the emergence of advanced information systems worldwide, shifting from traditional physical combat methods that rely on human intelligence toward a more complex, modern digital battlefield that combines the digital and physical worlds.

Cyber threats today do not easily fit within the traditional security framework prevailing in most modern states, which has driven the world's countries to adopt cyber-physical systems, a multidisciplinary field that combines embedded systems, control theory, networks, and physical processes. These systems are specifically designed for immediate interaction between the digital and physical worlds, physically blending single and multiple autonomous unmanned aerial vehicles, unmanned vehicles, smart weapon systems, and land and marine robots with advanced digital computing resources supported by Internet of Things technologies, artificial intelligence, and cybersecurity, in order to create a seamless, immediate system that enables armies to respond faster, more efficiently, and more precisely.

The military use of cyber-physical systems has today gone beyond the limits of traditional automation, bringing about a radical shift in how modern armies operate. With their capacity to enable independent decision-making, immediate responses, and improved coordination between defense systems, the future of warfare is increasingly dependent on modern technology.

In this regard, this study seeks to address cyber-physical systems from two angles: a conceptual angle that highlights the theoretical structure of the concept in the contemporary literature, and an applied angle that addresses the actual deployment of cyber-physical systems in the military domain, across both their cyber-digital and physical-material dimensions alike, with the aim of highlighting the technological and military integration in today's world.

Problem Statement:

How has the military use of cyber-physical systems gone beyond the limits of traditional automation in military defense, and to what extent do

these systems contribute to increasing efficiency, intelligent maneuver, and the effectiveness of military operations?

Study Objectives:

1. Defining the concept of cyber-physical systems and tracing its development in the contemporary literature.
2. Identifying and analyzing the structural layers that make up cyber-physical systems.
3. Examining the key characteristics that distinguish cyber-physical systems from traditional automated systems.
4. Assessing the adequacy of the conceptual framework for understanding the integration of cyber-physical systems into modern technological and defense applications.

Study Methodology:

The study adopts a descriptive-analytical methodology that combines conceptual analysis. It includes the analysis of technical reports and documented military practices in order to understand the dual functions (physical and cyber) of cyber-physical systems and their impact on modern defense systems.

Study Plan:

First Axis: Cyber-Physical Systems: The Conceptual Perspective in the Contemporary Literature

1. The concept of cyber-physical systems
2. The layers of cyber-physical systems

Second Axis: The Functions of Cyber-Physical Systems in the Military Domain

1. Uses of the physical/material system of cyber-physical systems in the military domain
2. Uses of the cyber/digital system of cyber-physical systems in the military domain

2. Cyber-Physical Systems: The Conceptual Perspective in the Contemporary Literature

2.1 The Concept of Cyber-Physical Systems

The concept of smart systems:

Smart systems are computer systems that use artificial intelligence and machine learning techniques to analyze data and then make decisions based on these analyses¹. They are essentially an evolution of microsystems, being an integrated mix of the components and technologies of microsystems such as cognitive science, microelectronics, nanoscience, mechanics, chemistry, biology, fluidic devices, optical devices, and other disciplines². These systems include a variety of tools such as machine learning, big data analysis, and artificial intelligence.

The roots of smart systems go back to the middle of the last century, with the emergence of the first approaches to automating devices and systems and connecting them to networks through three technologies (microelectronics, mechatronics/microsystem technology, and modern telecommunications technology) (see Table 1)³.

The concept of cybersecurity:

Cybersecurity is the ability to resist intentional and unintentional threats, and to respond and recover, thereby achieving freedom from danger or damage resulting from the disruption or destruction of information and communication technology, or from the misuse of information and communication technology. It requires protecting networks, computers, software, and data from attack, damage, or unauthorized access⁴.

The concept of cyber-physical systems:

Cyber-physical systems are engineered systems built on the seamless integration of computational algorithms and physical components⁵. Cyber-physical systems allow for the design and development of the next generation of aircraft and spacecraft, hybrid gas-electric vehicles, fully autonomous driving in cities, and prosthetic limbs that allow brain signals to control physical objects⁶.

As for the military domain, the design of military cyber-physical systems is a complex undertaking that encompasses numerous fields, such as the cyber domain, through software, control, computing, and communications, or the physical domain, such as the structural, mechanical, thermal, and so on (see Figure 1)⁷. Military cyber-physical systems are thus

integrated to meet the needs of military-specific missions, such as unmanned vehicles and weapon systems⁷.

2.2 The Layers of Cyber-Physical Systems

Cyber-physical systems operate on a three-level structure: the perception/physical layer, the data transmission/network layer, and the application/cyber layer⁸:

The first layer, the perception layer:

Also called the recognition layer or the sensor layer, devices in this layer have the ability to collect the real-time data needed for various purposes (such as monitoring and tracking), interpret what they receive from the physical world, and execute commands from the application layer. The data collected can include sound, light, mechanics, chemistry, heat, electricity, and biology⁹.

The second layer, the transmission layer:

Also known as the transport layer or the network layer, it is responsible for exchanging and processing data between the perception and application layers¹⁰.

The third layer, the application layer:

This is the most interactive layer, and its task is to process the information received from the data transmission level and issue commands to be executed by the physical units, sensors, and actuators¹¹.

3. Functions of Cyber-Physical Systems in the Military Domain

3.1 Uses of the Physical/Material System of Cyber-Physical Systems in the Military Domain

a. Unmanned Aerial Vehicles (Drones)

Drone networks play an integrating role between embedded systems, communication devices, computing capabilities, and control units. A drone network can build a closed loop consisting of data perception, information exchange, and decision-making through to final execution, closely integrating cyber operations into physical hardware. A drone network can therefore be considered a cyber-physical system¹². Drones are paired with the components of cyber-physical systems (communications, computing,

and control) and make optimal use of all available resources, thereby improving the performance of drone networks.

Unmanned aerial vehicles are seen as an indispensable part of the battlefield of the future. Not only can they proactively capture different kinds of information across a wide range of times and places (for example, border surveillance and intelligence reconnaissance), but they also help other unmanned and manned combat platforms complete dangerous missions (see Table 2)¹³.

Drones can also be classified into different categories: based on their size, into small or nano drones, small drones, medium drones, and large drones; and based on their flight range (see Figure 2)¹⁴.

b. Marine and Land Robots

The integration of computational elements with physical systems has led to the emergence of cyber-physical systems. These systems enable immediate interaction between the digital and physical worlds, with applications ranging from industrial automation and smart grids to self-driving vehicles, medical systems, and embedded and robotic systems. In parallel, mobile robots have advanced markedly, driven by progress in embedded computing, sensing technologies, and autonomous navigation algorithms¹⁵. To meet these requirements, robotic platforms are increasingly adopting the principles of cyber-physical systems to ensure flexibility, reliability, and ease of development.

c. Unmanned Underwater Vehicles in the Military Domain

Unmanned vehicles (meaning they operate without human intervention) function on land, at sea, and in the air, and are divided into two main types: autonomous/unmanned vehicles and remotely operated vehicles. Unmanned underwater vehicles are a self-propelled automated vehicle platform. Both autonomous vehicles and remotely operated vehicles are used in underwater search and rescue, underwater inspection of ship hulls, mapping, monitoring of marine habitats, and carrying out naval missions and scientific studies in deep ocean areas. Unmanned ground vehicles have been used as a key component in future naval operations missions such as mine countermeasures, maritime security, and naval blockade operations¹².

3.2 Uses of the Cyber/Digital System of Cyber-Physical Systems in the Military Domain

a. Military Artificial Intelligence

Military artificial intelligence systems are distinguished by their ability to process data more effectively than traditional systems. Thanks to their autonomous computing and decision-making capabilities, artificial intelligence also enhances the ability of combat systems to self-control, self-organize, and self-operate. Artificial intelligence is used today in almost all military applications, and the growing research and development support provided by military research agencies is expected to contribute to developing new and advanced AI-based technologies in the military domain.

b. Military Cybersecurity

Military cybersecurity is defined as an independent and specific branch of the broader concept of cybersecurity. In this context, cyber defense is viewed as part of state defense, guaranteed on the basis of a defense assurance law aimed at safeguarding sovereignty, territorial integrity, the principles of democracy, and the rule of law, and at protecting the lives and property of citizens from any external attack¹³.

Accordingly, the world's countries have come to recognize military cybersecurity as a planning and operational domain, and cyberspace was recognized at the NATO Warsaw Summit, held in July 2016, as the fifth operational domain (the fifth domain of warfare, no less important than land, sea, air, and space in military operations) in which NATO must defend itself and effectively deter adversaries¹³.

c. Military Internet of Things

The Internet of Things in defense is defined as a network of interconnected devices, systems, and technologies designed to collect, process, and exchange data in order to enhance military operations¹⁴. By integrating the Internet of Things into defense infrastructure, military institutions can improve decision-making, enhance situational awareness, and improve operational efficiency. The Internet of Things also links the physical/material and digital/cyber worlds, shortens distances, and enhances

responsiveness and intelligence across all sectors, especially the defense sector (see Figure 3) ¹⁴.

The Internet of Things in the military domain also provides the potential to improve efficiency, monitoring, and response in military and security operations (see Figure 4). It also enables improved effectiveness, monitoring, and response in military and security operations. This concept also refers to a network made up of interconnected physical objects that can exchange data over the internet.

CONCLUSION

In conclusion, this study shows that cyber-physical systems are no longer mere support tools, but have become essential components of modern military systems, thereby redefining operational logic, command effectiveness, and battlefield dynamics.

First: Findings

- Cyber-physical systems have gone beyond the constraints of traditional automation by enabling independent decision-making and immediate response.
- The close interaction between cyber and physical components has enhanced situational awareness and the coordination of military operations.
- The deployment of these systems contributes significantly to improving operational efficiency and the optimal use of resources.
- The growing use of cyber-physical systems reflects a structural shift in military doctrines toward models based on technologically advanced, intelligent warfare.

Second: Recommendations

- Strengthening the institutional and strategic frameworks governing the military use of cyber-physical systems to ensure their effective and responsible deployment.
- Investing in research and development to improve the resilience and security of military cyber-physical infrastructure.
- Developing specialized training programs to strengthen human skills in managing and overseeing these advanced systems.

5. Figures and Tables

5.1 Tables

Table 1. Technologies contributing to the development of smart systems

Technology	Its role in developing smart systems	Practical examples
Microelectronics	Electronics have transformed almost completely, now manufacturing small, precise circuits that allow for field-level computing. Microelectronic circuits are distinguished from traditional electronic circuits by two main features: integration and miniaturization.	<ul style="list-style-type: none">• Precision control units such as those found in remote controls.• Small computers such as Raspberry Pi/Arduino (e.g. a lighting-control robot).
Mechatronics and Embedded Systems	Allowed sensors, actuators, and software to be linked within a single coherent unit that performs physical functions (measurement, movement, control).	<ul style="list-style-type: none">• Unmanned ground robots (UGV), motor control systems.
Telecommunications / Networking	Decentralized data analysis has become a fundamental standard amid the tremendous progress in wireless communications; whereas the earliest smart systems transmitted their signals from one component to another exclusively by wire, today's modern communication standards allow for energy-efficient transmission over short distances.	<ul style="list-style-type: none">• Via Bluetooth LE technology, for example.• 4G/5G networks, field radio networks, satellite communications.

Table 2. Advantages and disadvantages of multiple drone systems versus single drone systems

Compared Features	Multiple Drone Systems	Single Drone Systems
Targeted coverage	Multiple drones can cover larger areas compared to single drones.	Can cover smaller areas.
Cost	Maintenance costs for multiple small drones are lower than the maintenance cost of a single large drone.	Large drones may not require high maintenance costs.
Mission time	The mission can be completed faster.	Mission completion is slower.
Radar cross-section	Requires a smaller radar cross-section.	Requires a larger radar cross-section.
Energy	Its system is energy-constrained.	Its system has greater energy capacity.
Network topology	Requires complex network topology.	Requires a direct and simple network connection.
Applications	A wide range of applications.	A limited range of applications.
Security	Has a larger attack surface and multiple attack vectors, especially when part of an IoT system.	Single systems are less exposed to attacks, but may represent a single point of failure if an attack succeeds.

5.2 Figures

Fig.1. The three components of cyber-physical systems

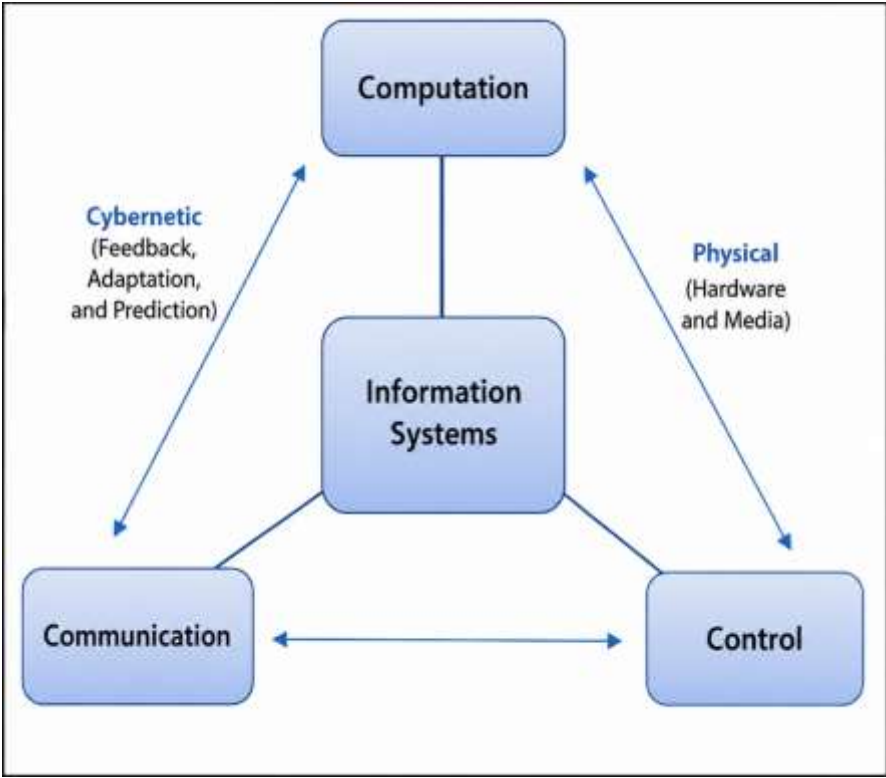


Fig.2. Classifications of drones

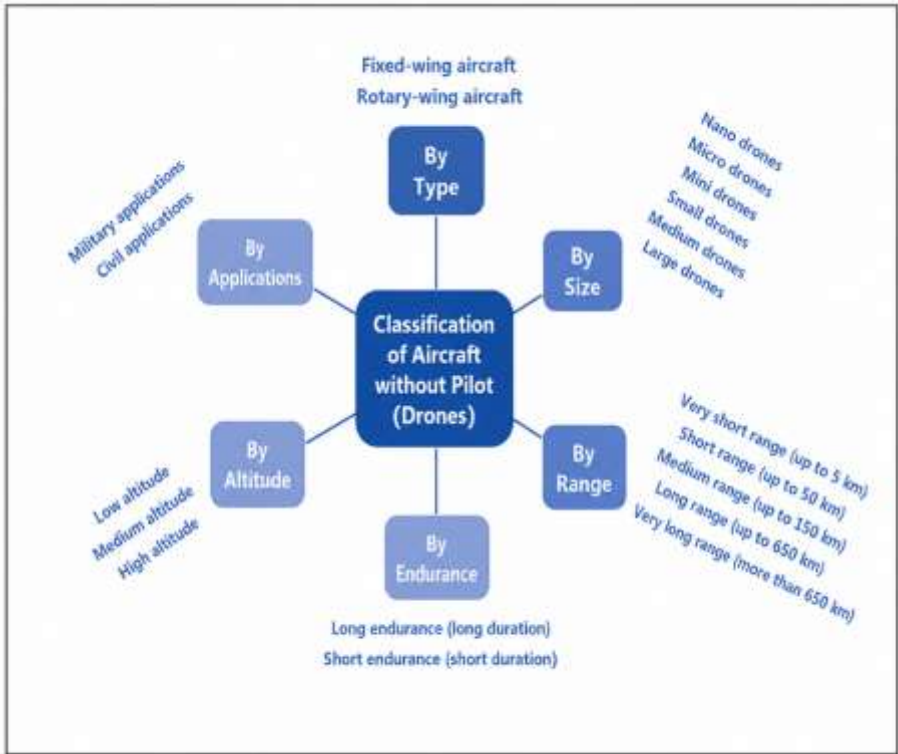


Fig.3. The difference in application between cyber-physical systems and the Internet of Things

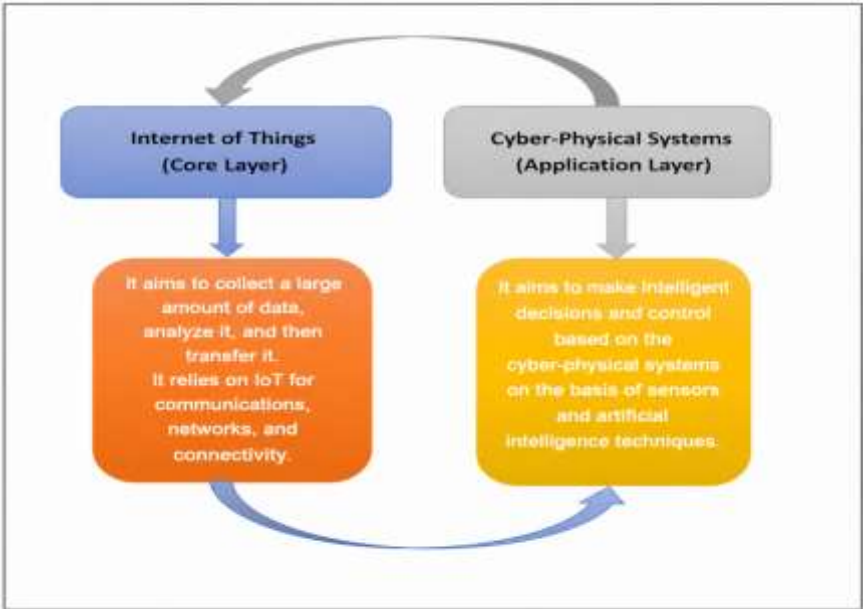
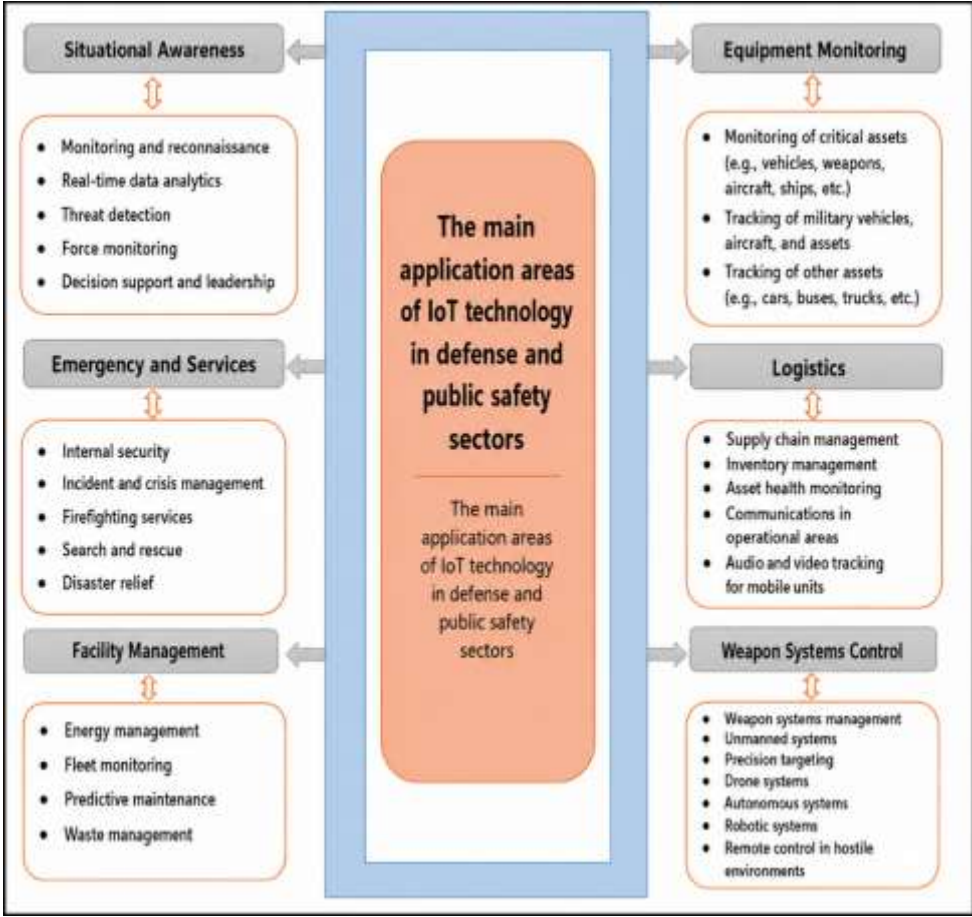


Fig.4. Areas of application of the Internet of Things in military defense



¹ Al-Naqeeb, A. (2024). Using smart systems to evaluate the impact of exchange rate changes on planning budget assumptions: A proposed approach to achieve financial sustainability. *Scientific Journal of Administrative and Financial Studies and Research*, 16(Special Issue), 101.

² QhalA, E. M. A. (2023). The role of smart systems in enhancing the performance of knowledge management in libraries based on the adoption of expert systems and robots. *International Journal of Professional Business Review*, 8, 1–28, p. 25.

³ Vogel, M. (2013). Smart systems: At high speed into an exciting future. *Silicon Saxony*. <https://silicon-saxony.de/en/smart-systems-at-high-speed-into-an-exciting-future/>

⁴ Fares Al-Amirat, *Cybersecurity the Concept and the Challenges of the Era*, Dar Al-Khalij for Publishing and Distribution, Amman, 2022, p. 25.

⁵ Bjorn Andersson, 2016.

-
- ⁶ Baheti, R., & Gill, H. (2011). *Cyber-Physical Systems. The Impact of Control Technology*, IEEE Control Systems Society, USA.
- ⁷ Uppal, R. (2022). DARPA SDCPS & JARVIS developing AI assisted design of military cyber physical systems. International Defense Security & Technology (IDST). <https://idstch.com/technology/ict/darpa-sdcps-jarvis-developing-ai-assisted-design-of-military-cyber-physical-systems/>
- ⁸ Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*
- ⁹ Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications and key challenges. 10th International Conference on Frontiers of Information Technology (FIT 2012), 2012, IEEE, Pakistan.
- ¹⁰ Zhang, B., Ma, X., & Qin, Z. (2011). Security architecture on the trusting Internet of Things. *Journal of Electronic Science and Technology (JEST)*, 9(4).
- ¹¹ Líšková, D., & A. J. (n.d.). A CPS-based architecture for mobile robotics: Design, integration, and localisation experiments. *Sensors*, 25(18), 2025.
- ¹² Hong, J., & Bae, I. (2023). Survey on the developments of unmanned marine vehicles: Intelligence and cooperation. *Sensors*, 23(10).
- ¹³ NÚKIB, 2018.
- ¹⁴ Singh, P. (n.d.). IoT in defence: How IoT is transforming defence systems and military operations. Hashstudioz. <https://www.hashstudioz.com/blog/iot-defence/>
- ¹⁵ Military Systems & Technology. (2025). How IoT is revolutionizing military operations. <https://www.militarysystems-tech.com/articles/how-iot-revolutionizing-military->