THE EVOLUTION OF NETWORK-CENTRIC WARFARE AND ITS IMPACT ON THE CONTEMPORARY SYSTEM OF INTERNATIONAL RELATIONS

DOI: 10.63407/738916

RUSTAM MAKHMUDOV
Associate Professor,University of World Economy and Diplomacy

Abstract *This article examines the evolution of network-centric warfare and its implications for contemporary military strategy, international relations, and the broader security environment. It argues that network-centric warfare represents a systemic transformation in the organization of armed forces, where military effectiveness increasingly depends on the integration of intelligence, command, and strike capabilities within unified information networks. The study examines the transition from asymmetric network-centric conflicts to emerging "network duels" between technologically advanced states operating competing digital and sensor-based military architectures. Particular attention is given to the growing role of satellite constellations, artificial intelligence, drone-centric operational models, and advanced command-and-control systems in shaping modern warfare. The article also considers the strategic consequences of technological diffusion and competition for critical resources, which are reshaping global power relations and creating new challenges for middle and smaller states. Finally, the study discusses the potential emergence of quantum network-centric warfare, integrating quantum communication, artificial intelligence, and autonomous platforms into a fully networked battlespace.*

Keywords *Network-centric warfare, revolution in military affairs, the Fourth industrial revolution, machinic phylum, military machine, security, international relations*

Introduction

At the beginning of the twenty-first century, the international system entered a phase of profound transformation driven by the rapid development of technologies associated with the Fourth Industrial Revolution. Digitalization, artificial intelligence, robotics, unmanned and autonomous systems, big data, cloud and quantum computing, as well as cyber and space technologies are exerting a systemic impact not only on the economy and the social structure of states, but also on the nature of military power as a key instrument of international politics. The changes currently taking place provide grounds to argue that the world has entered the new Revolution in Military Affairs (RMA), which is based on the principles of network-centric warfare.

The new RMA is directly affecting the system of international relations, leading to a redistribution of the global balance of military power, in which technological superiority now plays an equal role or even surpasses traditional quantitative indicators of a country's military potential. Emerging military technologies are also lowering the threshold for the use of force, as remote and unmanned means of warfare reduce the political and social costs of military operations.

Within the framework of the network-centric RMA, a revival of the logic of classical realism in international relations theory can be observed. Despite the widespread discourse on interdependence, institutional regulation, and "soft power," military power and a state's ability to control emerging technological domains are once again becoming decisive factors of international status and security. Network-centric warfare reinforces the role of the state as the central actor responsible for the mobilization of resources, the development of the defense-industrial complex, and the strategic management of technological sovereignty. The international system is increasingly returning to a condition of great-power competition, in which the balance of power is shaped not only by the size of armed forces but also by control over critical technologies.

Theoretical Conceptualization of the Network-Centric Revolution in Military Affairs

The emergence of breakthrough military technologies became an object of systematic scholarly inquiry in the early modern period. A notable example is the work of the military historian Michael Roberts, who introduced the concept of the "military revolution." His studies focused on the military reforms in seventeenth-century Sweden that temporarily transformed the country into a major European power and stimulated military reforms across Europe. Roberts paid particular attention to the introduction of light field artillery under the Swedish king Gustav II Adolf (1594–1632), which fundamentally altered the conduct of warfare. This transformation was later reinforced by the invention of the bayonet, the introduction of linear infantry tactics and regular armies. (Nefedov, 2010, pp. 36–40)

One of the earliest scholarly works addressing network-centric warfare is the book "War in the Age of Intelligent Machines" by the Mexican-American philosopher Manuel DeLanda. In order to explain how contemporary forms of warfare differ from earlier ones, he introduces the concepts of the "machinic phylum" and the "war machine."

According to DeLanda, the machinic phylum represents a universal principle underlying all self-organizing processes - from biological and chemical reactions to social systems and military formations. The concept identifies patterns through which order emerges from chaos, including phenomena such as emergence, phase transitions, and the cooperation of heterogeneous elements. The phylum is not an object in itself; rather, it reveals the fundamental relationship between chaos and structure, historically manifesting itself through weapons systems, military tactics, and the organization of armies (DeLanda, 2014, pp. 35–36).

In turn, the "war machine" represents a particular form of an emergent system that arises under conditions of extreme instability - whether social, economic, political, or religious. Such systems function as points of assemblage. A war machine emerges when previously disparate elements - fighters, units, weapons, and tactical practices - reach a critical threshold and begin to cooperate, forming a unified and organized whole. A key characteristic of the war machine is its capacity to adapt to changing battlefield conditions, reconfigure the structure of units, and modify tactical patterns of action.

War machines manifest themselves across four levels: technical support of warfare, the tactical level, the strategic level, and logistics, which represents the highest level of the hierarchy. At the first level, military technologies and weapons systems are developed; at the second level, the organization of combat operations is formed; at the third level, strategic planning and the political objectives of the state or society are articulated; and at the fourth, logistical level, the art of supply and support is realized.

DeLanda pays particular attention to this fourth level, arguing that highly organized military logistical systems generate new forms of interaction and behavioral patterns within the armed forces. Logistics determines not only the capacity to move supplies and information but also the overall efficiency, adaptability, and coordination of the war machine across different historical periods (DeLanda, 2014, pp. 40-41).

Manuel DeLanda argues that each level of the war machine is governed by its own specific "laws," and that the task of the commander-in-chief is the "discovery and application of the laws of each level in order to create an interconnected whole". DeLanda also emphasizes that the effectiveness of a war machine depends directly on the degree to which the machinic phylum is able to pass through it. As he notes, "the task generals have always faced is to ensure that the machinic phylum 'flows through' the levels of weaponry, tactics, strategy, and logistics" (DeLanda, 2014, p. 41).

The Mexican-American philosopher illustrates this idea through three types of early modern and modern armies: the clockwork army, the motorized army, and the network army.

The clockwork armies of the seventeenth to early nineteenth centuries were highly centralized, characterized by low mobility and oriented toward wars of attrition, which indicates a relatively weak transmission of the machinic phylum. These armies reflected the socio-political structure of the societies of that time, in which the authority of the monarch occupied a central position (DeLanda, 2014, p. 108).

The motorized army of the nineteenth and twentieth centuries represented a decisive step toward a more effective integration of the machinic phylum. This was manifested in the emergence of well-trained and loyal national armies supported by professional intelligence and staff structures. Although the centralized socio-political system remained intact in the form of the nation-state, it became increasingly capable of adapting its functioning to changes in the external environment. It should be noted that the motorized army became possible due to the phenomenon of the industrial revolutions. The invention of the internal combustion engine, the use of oil, and the introduction of assembly-line production during the Second Industrial Revolution gave a powerful impetus to the further development of military affairs and significantly improved the transmission of the machinic phylum.

Finally, according to DeLanda, the machinic phylum manifests itself most fully in the network army - a decentralized form of military organization whose effectiveness is determined by initiative at the local level. This initiative is associated with the ability of combatants to assess the operational environment using interactive information systems and communication technologies. In DeLanda's interpretation, such a model of warfare could ultimately reduce the very likelihood of war itself.

Parallel to the work of philosophers on military revolutions during the 1990s, the same issue was also at the center of attention among military theorists who were developing the concept of network-centric warfare. A key contribution to the theoretical foundations of network-centric warfare was made by the U.S. Navy vice admiral Arthur Cebrowski, Pentagon analyst John J. Garstka, and Admiral Jay L. Johnson in the late 1990s. Their concept represented a major turning point in military thought during the transition to the digital era. The main principles of the new theory were outlined in their article "Network-Centric Warfare: Its Origin and Future".

Analyzing network-centric warfare, the authors proceed from the fundamental premise that there exists a structural relationship between the mode of wealth production and the mode of warfare. According to their argument, states wage war in much the same way as they generate economic power, since in both cases the decisive role is played by dominant organizational and technological principles. In a context where information technologies have radically transformed the nature of economic competition, these same transformations inevitably reshape the conduct of warfare. Therefore, the general logic of the ongoing Revolution in Military Affairs can be understood through the analysis of contemporary economic processes.

Arthur Cebrowski and John J. Garstka construct their explanation through a contrast between two models of economic organization. The first, conventionally referred to as "Economy A," corresponds to the industrial logic of decreasing returns on investment, relative market stability, and the substitutability of goods and services. Within this model, competition tends to lead to equilibrium, while increases in market share are accompanied by rising costs and declining efficiency.

The second model - "Economy B" - emerges under conditions of the dominance of information technologies and is characterized by increasing returns, the absence of stable market equilibrium, and the presence of technological lock-in effects. In such an environment, the winner gains disproportionately large advantages, while competitors are gradually pushed out of the system.

The key mechanism of Economy B is the network effect, whereby the value of a system grows as the number of participants increases, while the dominant standard forms an ecosystem from which exit becomes economically and organizationally disadvantageous. Historical examples of technological lock-in -

from the QWERTY keyboard standard to the victory of VHS over Betamax and the formation of the Wintel ecosystem - demonstrate that competition in such an environment takes on a nonlinear and asymmetric character. Victory is achieved not so much through the superiority of a single product as through control over the architecture of interactions, technological standards, and information flows.

It is precisely this logic that Arthur Cebrowski and John J. Garstka transfer to the sphere of military affairs. In their conception, network-centric warfare is intended to reproduce the effects of increasing returns and structural dominance characteristic of the new economy. The objective is not merely to enhance the efficiency of the armed forces, but to create an information-operational environment in which the adversary is excluded from the full command, intelligence, and decision-making cycle. As in "Economy B," victory is achieved through the capture of standards, speed, interoperability, and network density, rather than solely through the physical destruction of the enemy's forces.

Thus, network-centric warfare represents not simply a technological innovation but a transformation in the organizational principle of warfare. It is oriented toward achieving a lock-in effect, whereby the adversary loses the capacity to operate effectively within the dominant system. In this sense, the military revolution described by Cebrowski and Garstka reflects broader structural changes associated with the Fourth Industrial Revolution and indicates a transition of warfare into the realm of competition for control over networks, technological standards, and architectures of interaction.

From a technological perspective, researchers note that network-centric warfare became possible not only as a result of changing principles of competition but also due to a fundamental shift in information technologies - from a platform-centric computing model to network-centric computing. Platform-centric computing emerged during the era of widespread personal computer adoption and assumed the relative autonomy of computing systems, each oriented toward a single device or software platform. However, extensive IT sector investment in research and development led to the emergence of technologies that created conditions for a radical transformation of this model.

In the new technological environment, value is generated not by individual computing devices but by their integration into a network, where intensive and rapid information exchanges among numerous nodes produce effects unattainable for isolated systems. This principle has been formalized in economics through Metcalfe's Law (Cebrowski & Garstka, January 1998).

According to this law, the value of a network grows disproportionately with the number of its participants, because each new node (participant) increases not only its own utility within the network but also the number of possible interactions among all other nodes. Each new participant connects not to a single hub but to all other nodes simultaneously, thereby sharply increasing the total number of potential interactions. By "disproportionate growth," it is meant that the value of the network increases faster than linearly as the number of participants grows.

Unlike isolated systems, where value is determined by the characteristics of individual elements, in networks the decisive source of power is the connections, i.e., the interactions themselves rather than the elements. As the number of nodes increases, the potential interactions grow according to a quadratic principle:

1 node – 0 interactions;

2 nodes – 1 possible connection;

3 nodes – 3 connections;

10 nodes – 45 potential connections;

100 nodes – 4,950 connections.

This is why networked structures - in economics, technology, and network-centric warfare - can rapidly accumulate advantages, producing dominance effects, accelerating decision-making, and displacing alternative models.

The article notes that changes in economic logic and the technological base have led to a transformation of organizational forms. Companies began to view themselves not as autonomous hierarchies but as components of large, adaptive, and learning ecosystems, in which competition and cooperation are intertwined and the key resource is information. High situational awareness, minimal decision-making delays, and the capacity for self-organization have allowed such structures to achieve sustainable competitive advantages.

It is against this backdrop that the concept of network-centric warfare emerges. According to the network-centric warfare theorists, the military domain cannot remain tied to a platform-centric model when the very nature of the competitive environment has changed. If economies and technologies have shifted to a network logic, warfare must inevitably be reimagined in the same terms.

Network-centric warfare entails a transition from the dominance of individual platforms to the dominance of networks of interacting elements. Military power, in this context, is determined not by the quantity or specifications of weapons systems but by the quality of connectivity, the speed of information exchange, and the ability of distributed forces to act in a coordinated manner. A central condition for this transition is information superiority, understood as the possession of relevant, accurate, and timely information rather than merely a large volume of data.

Operationally, network-centric warfare relies on the establishment of a unified network architecture, which includes a high-performance Information Grid, Sensor Grids that generate a common operational picture of the battlespace, and Engagement Grids that translate situational awareness into combat actions. The interaction of these elements produces an effect in which the whole exceeds the sum of its parts, with the speed and density of interactions becoming a source of new combat power.

A key outcome of such a system is speed of command - the ability to convert information superiority into decisive advantage by radically shortening decision-making cycles and imposing unfavorable conditions on the adversary even before its strategy can be deployed. Under these conditions, warfare ceases to be a sequence of discrete phases and instead becomes a continuous, high-tempo process in which the opponent is deprived of operational pauses.

An additional mechanism is self-synchronization - the ability of well-informed units to coordinate actions from the bottom up within the framework of the commander’s intent, without constant directive control. This capability overcomes the limitations of traditional hierarchical structures and significantly enhances the effectiveness of combat power deployment (Cebrowski & Garstka, January 1998).

Ultimately, network-centric warfare marks a shift from attrition-style warfare to effects-based warfare, in which the decisive factor is not the mass of forces but the tempo of change and the ability to manage a complex adaptive system. Similar to the logic of increasing returns in Economy B, network-centric warfare creates conditions in which the rapid seizure of initiative leads to nonlinear advantages and the disruption of the adversary's strategy at the early stages of a conflict. In this sense, network-centric warfare is regarded as one of the most profound revolutions in contemporary military affairs.

The further evolution of military thought in the domain of network-centric warfare led to the development of two additional concepts: the "kill chain" and the OODA loop. According to Maj. Gen. Sudhakar Jee, "The kill chain is the systematic process from identifying a target to destroying it." He notes that the military employs the F2T2EA model: Find, Fix, Track, Target, Engage, and Assess. The kill chain concept allows for a significant reduction in the time from target identification to engagement and situational assessment - from hours or even days in traditional warfare to mere minutes or seconds (Jee, 2025, August 13).

The concept of the OODA loop - Observe, Orient, Decide, Act - developed by American military strategist Colonel John Boyd, emphasizes that the actor who completes their OODA loop faster gains a decisive advantage while simultaneously disrupting the adversary's loop (Jee, 2025, August 13).

Practical Implementation of the Network-Centric Warfare Concept

New network-based approaches to the theory of combat operations have had a fundamental impact on the emergence of a new Revolution in Military Affairs (RMA) and, consequently, on the transformation of the entire system of international relations and security. Since the early 2000s, a state's ability to organize its armed forces and conduct military operations based on the principles and methods of network-centric warfare has increasingly become a key criterion determining its position within the international system.

As a result of this transition into the modern digital era, the international community has come to recognize a new classification of states as actors in international relations. This classification includes three types of states:

- States possessing predominantly motorized armies;

- States with network-centric military structures;

- Hybrid states with partially network-centric or hybrid armies.

This classification, in turn, has defined the types of military conflicts in the digital age, which are situated between two poles: asymmetric network-centric warfare, or "network army vs. motorized army," and symmetric network-centric warfare, or "network-on-network duels."

The first conflict in which the concept of network-centric warfare was practically tested was the U.S. and U.K. military operation against Iraq, codenamed "Shock and Awe" in 2003. In this operation, the American networked army faced the motorized forces of Iraq. The U.S. strategy implemented the doctrine of "Rapid Dominance," developed in 1996 by military analysts Harlan K. Ullman and James P. Wade specifically for the National Defense University. The core principle of this doctrine is to achieve instantaneous strategic superiority by delivering such a powerful and rapid strike against the adversary's command systems, infrastructure, and military potential that it disrupts the decision-making process, thereby paralyzing the will to resist and producing a psychological effect of shock and demoralization.

"To achieve this result, 'Rapid Dominance' must control the operational environment and, through that superiority, control what the adversary perceives, understands, and knows, as well as control or regulate what is not perceived, understood, or known," write the American analysts (Ullman & Wade, 1996, pp. 11-16).

The emergence of new information technologies enabled the U.S. and U.K. to combine network-centric warfare with the Rapid Dominance doctrine. In the initial phase, the allies achieved information and intelligence superiority through a multi-layered sensor network that included satellite reconnaissance, E-3 Sentry AWACS aircraft, Predator UAVs, ground reconnaissance units, and communications interception. This network created a unified information environment, transmitting real-time data to command centers.

At the same time, a networked integration of enemy weapons was implemented. For the first time, the principle of "sensor-to-shooter" was applied in real time. Targets were identified by sensors, with the data transmitted through the Global Information

Grid (GIG), allowing strike assets - aircraft, cruise missiles, and artillery - to engage targets without prolonged coordination cycles.

Experts note that the Americans effectively employed automated command and control systems, such as the Theater Battle Management Core System (TBMCS) for air operations management at the theater level, and Force XXI Battle Command Brigade and Below (FBCB2) for tactical command of forces across the brigade–battalion–company hierarchy (Leonkov, 2018, October 16).

Total information superiority enabled the U.S. and U.K. to maintain a high operational tempo and virtually eliminate operational pauses, thereby minimizing organizational frictions and allowing the flows of the war machine filum to circulate more freely within the military network. This fully corresponded to the principle of self-synchronization.

Advancing units - armored and mechanized formations - acted rapidly, relying not on top-down orders but on a real-time information picture. As a result, the Iraqi army, organized along a hierarchical principle, was unable to respond effectively to changing circumstances.

The network-centric model allowed the U.S. to maintain continuous pressure on Iraqi forces. Strikes by American and British forces were delivered simultaneously against command centers, communications nodes, and infrastructure, producing an effect of system-wide disruption. The hierarchical command structure of the Iraqi military collapsed within the first few days, generating the intended effect of "shock and awe."

This triumph of the United States marked the beginning of an era of its unquestioned power dominance in international politics. However, as history has often shown, the emergence of a new Revolution in Military Affairs triggered an arms, technology, and knowledge race, reshaping the entire landscape of global politics, security, economics, investment flows, and scientific thought.

It should be noted that network-centric warfare can serve as a striking example of "technological diffusionism," the essence of which lies in the idea that any technological discovery occurs only once within a particular culture and subsequently begins to spread or be adopted by other societies, forming a cultural cycle (Nefedov, 2011, pp. 47–73).

Despite the controversial nature of this theory, the era of technological warfare, which began after the First Industrial Revolution, provides clear examples of technological diffusionism. Innovations in technology and military affairs developed in the West were eventually adopted by non-Western cultures as part of catch-up modernization and Westernization, often for survival and strategic adaptation.

One of the first countries to demonstrate catch-up development in the field of network-centric warfare was Russia, which in 2014 established the high-tech National Defense Management Center and the Aerospace Forces (VKS). For operational-strategic command, the Akatsiya-M system was implemented, integrating information flows from various command structures. At the operational-tactical level, the Sozvezdiye-M2 and Andromeda-D systems were deployed, enabling command and control of ground and airborne troops. This architecture allowed the integration of intelligence data from satellite systems, unmanned aerial vehicles, and ground units (Leonkov, 2018, October 16). The network-centric warfare methods were first practically tested in Syria in 2015 against terrorist organizations such as ISIS and Jabhat al-Nusra. However, this remained an asymmetric form of network-centric warfare.

The first instance of a “network-on-network duel” can be considered the military operations between Russia and Ukraine, which are currently being closely studied by military specialists. Beginning in February 2022 as conventional clashes between motorized armies, the conflict gradually transitioned into a network-centric form, which has been termed drone-centric warfare. Despite an initially significant disparity in military power favoring Russia, the conflict evolved into a phase of protracted combat, largely due to Ukraine establishing its own network-centric warfare architecture, incorporating multiple integrated components.

At its core lies the principle of kill chains: “Battlefield victory hinges on whose kill chain is faster.” From a technical perspective, the central element is the Delta Situational Awareness and Battlefield Management System, which integrates intelligence data and manages operations in real time.

The second key component of the Ukrainian network-centric warfare model is the drone-centric operational architecture, in which unmanned systems perform reconnaissance, targeting, and strike functions. The mass deployment of thousands of UAVs creates a distributed network of sensors and strike platforms, integrated into a unified reconnaissance–strike complex. These drones enable the implementation of the sensor-to-shooter principle.

In 2024, Ukraine established a new branch of the armed forces—the Unmanned Systems Forces (USF) - which integrates aerial drones, ground robotic systems, and maritime surface and subsurface drones into a single operational structure (Samus, 2025, January 15).

A critical role in the Ukrainian model of network-centric warfare is played by access to Starlink - a global broadband satellite system developed by the American company SpaceX. It is based on a large constellation of satellites in Low Earth Orbit (LEO), providing high-speed internet access virtually anywhere in the world. Starlink can be considered an infrastructure channel for the circulation of the war machine filum's information flows within the modern military system. Through Starlink, the effect of a "military assemblage" is achieved—linking heterogeneous technological elements into a unified network architecture.

Russian NCW technology has also continued to evolve. In 2025, the Unmanned Systems Forces were established within the Russian military (RBC, 2025, November 28). Satellite communication systems such as Kvadrat - for transmitting large volumes of information at the regimental and divisional level - and Sprint, which ensures stable connectivity for command posts, were developed (Grigorenko, 2025, September 14). For the first time in the world, Moscow integrated hypersonic missiles and the medium-range ballistic missile Oreshnik into a single networked command architecture, enabling instantaneous coordination between intelligence, command, and strike assets.

The second contemporary instance of a network-on-network duel was the brief military conflict between India and Pakistan, which lasted from April 24 to May 10, 2025. From the perspective of conventional weaponry, Delhi traditionally held an indisputable advantage over Islamabad. However, Pakistan's application of network-centric warfare elements largely neutralized this advantage. Of particular interest is the analysis of the conflict by Maj. Gen. Sudhakar Jee.

According to him, during Operation Bunyan-ul-Marsoos ("solid wall of lead"), Pakistan demonstrated an unexpected level of network-centric capabilities. "When Pakistan launched Operation Bunyan-ul-Marsoos, they demonstrated network-centric capabilities that surprised military analysts worldwide," he notes.

The primary reason for Pakistan's breakthrough, he argues, lies in the long-term technological integration with China. According to Maj. Gen. Jee, this integration was carried out in several key areas:

- The Pakistani armed forces gradually incorporated Chinese systems into a unified military network. "Chinese J-10C fighters with PL-15 beyond-visual-range missiles, HQ-9 air-defense systems, and sophisticated electronic warfare capabilities now operate within a unified Pakistani-Chinese network," observes the Indian military expert.

- During the conflict, China provided Pakistan with real-time intelligence via the BeiDou Navigation Satellite System and ground-based radar networks. This allowed Pakistani forces to track Indian air force movements and coordinate defensive actions with high precision.

- The integration of Swedish SAAB 2000 Erieye early-warning aircraft with Chinese combat platforms created comprehensive air-situation awareness that matched anything India possessed.

As a result, Pakistan will shorten decision cycles and operate within the Indian OODA loop. "They achieved multi-domain coordination across air, land, and cyber domains simultaneously. Most concerning, they integrated kinetic operations with cyberattacks, targeting over 1.5 million Indian digital infrastructure components. And soon, we are going to witness the integration and dominance of China-Pakistan collaboration across six domains - air, land, sea, cyber, space, electromagnetic spectrum," the Indian expert concludes.

Although India also employed principles of network-centric warfare (NCW) during the conflict, relying on relatively effective systems such as the Integrated Air Command and Control System (IACCS), which provides centralized air defense management, and the Defence Communication Network (DCN), Maj. Gen. Sudhakar

Jee notes that several limitations were identified in India's network-centric architecture.

First, there were persistent problems with inter-service integration. The army, navy, and air force each operate their own communication networks, which can exchange information but do not ensure full real-time data sharing. This fragmentation reduces the speed of information flow and hinders the effectiveness of networked operations.

Second, battlefield-management systems have dangerous gaps – although Army headquarters can access satellite imagery and intelligence on developments along the LAC, this information does not reach frontline troops in real time. These intelligence assets remain available only to higher headquarters located kilometers behind the front lines.

Third, a significant issue remains technological dependence on foreign components. Many communication systems and unmanned platforms incorporate foreign hardware and software. Instances of hacking of Indian military drones revealed the presence of Chinese components with potential backdoors, creating vulnerabilities for enemy interference and potentially disrupting the kill chain in critical situations (Jee, 2025, August 13).

The military operations launched on February 28, 2026, by the U.S. and Israel against Iran marked a significant event, as Washington—the originator of network-centric warfare - faced a network-on-network duel against the Iranian military for the first time. For the U.S., accustomed after operations in Iraq and Libya to its near-total military-technological superiority, Iran's capability to conduct network-centric warfare came as a complete surprise.

Whereas during the 12-day war of 2025 with Israel the Iranian military primarily sought to deliver massive strikes using ballistic and hypersonic missiles and drones, the 2026 conflict demonstrated a completely different tactical and strategic level: the Islamic Republic executed precision strikes against American military assets in the Gulf region. The primary goal was not merely the physical destruction of targets, but the disruption of critical nodes in the adversary's infrastructure, such as military bases, command centers, communications, and ports. For instance, by March 7, 2026, four radars of the AN/TPY-2 missile defense system in Jordan, the UAE, and Saudi Arabia had been neutralized, as well as the fixed AN/FPS-132 early warning radar in Qatar (Trevithick & Rogoway, 2026, March 7).

The destruction of nodes reduces network conductivity, impairing the U.S.'s ability to rapidly collect, process, and transmit intelligence, as well as to coordinate strike forces. Consequently, the loss of nodes and slowed information flows renders the U.S. network-centric command system less effective, limiting its ability to impose networked will on the adversary.

A distinctive feature of Iran's technological engagement with the U.S. and Israel was the use of artificial intelligence and data centers, which accelerate the processes of information processing and target selection. In this context, the attacks by the Islamic Revolutionary Guard Corps on three Amazon data centers - two in the UAE and one in Bahrain - appear deliberate. The official explanation was that these data centers were supporting the US military operation (Palmer, 2026, March 4). In modern warfare, data centers effectively constitute strategic military assets, their role comparable to air bases, satellites, and air defense systems.

Thus, the transition of network-centric warfare into the era of "network duels" has elevated the art of war to an unprecedented level and posed a series of critical challenges for large and medium-sized states, the impact of which on the international system and security is already becoming significant.

First, the development of a networked army is becoming an inescapable stage in the evolution of armed forces. The ongoing military revolution is, in terms of significance, comparable to the historical transition from bows and crossbows to firearms, and states that fail to adopt new technologies will rapidly lose their strategic advantage.

Second, the shift to a network-centric model requires the creation of a self-sufficient research and production cycle to minimize dependence on imported technologies and reduce the risk of backdoors - hidden vulnerabilities that could grant external actors control over the military network. An independent technological base ensures full control over network architecture, command algorithms, and intelligence assets. For small and medium-sized countries, establishing a fully independent network-centric warfare industry, encompassing AI and data analysis algorithms, satellite reconnaissance, cloud infrastructure and data centers, microelectronics, cybersecurity, and defense software, will be extremely challenging, as it demands substantial investments and time.

Third, the creation of a proprietary satellite constellation is a necessary condition for maintaining a continuous flow of intelligence, navigation, communications between units, and command and control across all operational levels. Without a robust satellite network, conducting network-centric warfare is impossible.

The United States currently remains the leader in low-orbit satellite superclusters thanks to Starlink. However, China plans to challenge U.S. dominance in the near future. In early 2026, Chinese companies submitted applications to the International Telecommunication Union (ITU) for the deployment of over 200,000 internet satellites in Low Earth Orbit (LEO) (Denisenko, 2026, January 13). Efforts by Iran should also be noted, as it seeks to establish its own LEO constellation. In December 2025, three Iranian satellites were launched into low Earth orbit with Russian assistance (Iran International, 2025, December 22). By the end of March 2026, the launch of an additional 20 satellites, referred to as the Soleimani constellation, was planned to provide narrowband communications aimed at developing Internet of Things (IoT) services (Iran International, 2025, August 19).

As with the creation of a fully independent network-centric warfare industry, building a satellite constellation can be an extremely challenging task for resource-constrained states, potentially driving them toward military-technical alliances to enable joint development and the sharing of critically important data.

Fourth, the development and evolution of artificial intelligence (AI) is essential. In network-centric warfare, AI becomes indispensable as it reduces the kill chain cycle and enables the simultaneous management of a large number of intelligence and strike platforms. This has not only technological but also ethical implications for the international system. In the context of network duels, where international law is effectively destabilized, ethical concerns often become secondary. Competing states aim to maintain or gain strategic superiority, and thus may sacrifice traditional norms of warfare to enhance the effectiveness of automated systems. As the Guardian editorial board notes: "The pace of AI-driven warfare means that caution can look like handing control to adversaries."

Fifth, network-centric warfare requires sustained access to critical resources and raw materials for next-generation technologies, including rare-earth metals, high-purity chemical compounds, materials for quantum and hypersonic systems, fuels for satellites and autonomous platforms, and components for microelectronics and sensors. Lack of access to these resources prevents the development of a self-sufficient technological base, increases dependence on external suppliers, and heightens vulnerability of networked infrastructure. In the context of network duels, these material nodes are critical for maintaining the flow of the machine phylum and executing strategic plans. Naturally, the struggle for control over these critical materials is already reshaping the international geopolitical landscape.

Conclusion

In conclusion, it should be noted that network-centric warfare has become a key stage in the evolution of modern military affairs, elevating the historical tendencies of maneuverability, distribution, and adaptability of armed forces to a systemic level. The power of an army is now determined not only by the number of combat platforms it possesses, but also by its ability to function as a unified, self-synchronizing information network, where information superiority and the speed of decision-making become decisive factors of success. The examined examples of "network duels" clearly demonstrate that states capable of integrating intelligence, command, and strike assets into a single networked architecture gain a strategic advantage that remains inaccessible to traditional motorized armies.

At the same time, the development of network warfare will not be limited to the current level of information and automated technologies. The next stage of its evolution, and possibly a new revolution in military affairs, may emerge in the form of quantum network-centric warfare, a technological breakthrough that many analysts expect to materialize around 2040.

Future quantum network-centric warfare will shape a fundamentally new paradigm of armed conflict. It will integrate physical, cybernetic, and biotechnological domains, as well as nano-enabled technological platforms, into a single, fully integrated battlespace in which the speed, precision, and security of networks reach previously unattainable levels.

This transformation will continue to fundamentally reshape the system of international relations. Major powers will seek to develop their own quantum network capabilities, while middle and smaller powers will face a strategic choice: either invest in the independent development of network infrastructures or join military-technological alliances in order to gain collective access to critical resources, satellite constellations, and artificial intelligence infrastructures.

Overall, understanding and mastering the principles of network-centric and quantum network-centric warfare is becoming a key competence for future military specialists. It requires a deep understanding not only of traditional military concepts but also of the principles of quantum communication, autonomous systems, data analytics, and comprehensive information security. The emerging era of “network duels” and the transition toward quantum battle architectures demonstrate that armed conflicts in the twenty-first century will increasingly be determined by the speed, connectivity, and integration of networks, rather than solely by the numerical strength of armed forces or traditional firepower.

References

1. Cebrowski, A. K., & Garstka, J. H. (1998, January). Network-centric warfare: Its origin and future. Proceedings, 124(1), 1,139. https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future
2. DeLanda, M. (2014). Voyna v epokhu razumnykh mashin. Yekaterinburg; Moscow: Kabinetny Uchenyy; Moscow: Institute of Public Humanities Research.
3. Denisenko, A. (2026, January 13). Kitay zapustit 200 tysyach internet sputnikov, chtoby obygrať Starlink i zanyat mesto na orbite. CNews. https://www.cnews.ru/news/top/2026-01-13_kitaj_planiruet_zapustit
4. Grigorenko, D. (2025, September 14). Svyazisty razvernuli novye sputnikovye kompleksi na ucheniyakh “Zapad-2025”. Vzglyad. https://www.vz.ru/news/
5. Iran International. (2025, August 19). Iran plans maiden launch of its first satellite constellation by March. Iran International. https://www.iranintl.com/en/202508192267
6. Iran International. (2025, December 22). Iran set to orbit three satellites in joint launch from Russia. Iran International. https://www.iranintl.com/en/202512224276
7. Jee, S. (2025, August 13). Network-centric warfare: Pakistan’s edge and India’s wake-up call. Indus International Research Foundation. https://indusresearch.in/home-opinion-network-centric-warfare-pakistans-edge-and-indias-wake-up-call-by-maj-gen-sudhakar-jee-retd/
8. Leonkov, A. (2018, October 16). Nash asimmetrichnyy otvet na amerikanskie “setetsentricheskie voyny”. Zvezda Weekly. https://zvezdaweekly.ru/news/20181041654-460kh.html

9. Nefedov, S. A. (2010). Istoriya Rossii. Faktorny analiz. T. II. Ot okonchaniya Smuty do Fevralskoy revolyutsii. Vol. II. Moscow: Territory of the Future Publishing House. (University Library of Aleksandr Pogorelsky series).
10. Nefedov, S. A. (2011). Petr I: Blesk i nishcheta modernizatsii. Istoricheskaya Psikhologiya i Sotsiologiya Istorii, 1, 47–73. https://www.socionauki.ru/journal/files/ipisi/2011_1/petr_I_blesk_i_niweta_modernizacii.pdf
11. Palmer, A. (2026, March 4). Amazon’s Bahrain data center targeted by Iran for support of U.S. military, state media says. CNBC. https://www.cnbc.com/2026/03/04/amazon-bahrain-data-centers-targeted-iran-drone-strike.html
12. RBC. (2025, November 28). Voiska bespilotnykh sistem: chto eto za novyy rod voysk i zachem ego sozdali. RBC. https://www.rbc.ru/base/28/11/2025/6929ade89a79473dcdbbc7b8?utm_referrer=https%3A%2F%2Fwww.google.com%2F
13. Samus, M. (2025, January 15). Russia’s war in Ukraine: Drone-centric warfare. The International Centre for Defence and Security (ICDS). https://icds.ee/en/russias-war-in-ukraine-drone-centric-warfare/
14. Trevithick, J., & Rogoway, T. (2026, March 7). Iranian attacks on prized missile defense radars are a wake-up call. The War Zone. https://www.twz.com/news-features/iranian-attacks-on-critical-missile-defense-radars-are-a-wake-up-call
15. Ullman, H. K., & Wade, J. P. (1996). Shock and awe: Achieving rapid dominance. Washington, DC: National Defense University.