



Beyond the Land Domain: Is Cyber the New Front of Modern Warfare?

Published on 15/10/2026

For centuries, military superiority was determined primarily by the ability to seize and maintain control of territory. Armies faced one another on the ground, offensives aimed to occupy strategic positions, and the destruction of opposing forces was one of the main means of achieving victory. The evolution of air power, naval forces and, later, space capabilities progressively expanded the dimensions of conflict, without eliminating the centrality of ground operations.

Today, this balance is changing. Not because tanks, artillery, infantry and conventional assets have lost their importance, but because their effectiveness increasingly depends on technological infrastructure located outside the traditional battlefield. Command-and-control systems, satellite communications, computer networks, intelligence capabilities and digital platforms are now an essential component of military power.

An army may possess considerable numerical and technological superiority, yet see its operational capability compromised if an adversary succeeds in disrupting

communications, altering the flow of information or rendering unavailable the systems on which force coordination depends.

It is in this context that the Cyber domain has assumed a strategic role. Its distinctive feature lies not only in the ability to strike computer systems remotely, but also in its capacity to produce effects that can extend across all other operational domains. Cyberspace is not simply another environment in which to confront an adversary: it has become one of the infrastructures underpinning the entire functioning of modern Armed Forces.

From territorial conquest to information superiority

In July 2016, during the Warsaw Summit, NATO officially recognized cyberspace as an operational domain, alongside the land, air and maritime domains. In December 2019, space was also recognized as an operational domain, completing a framework that now encompasses five fundamental environments: Land, Air, Maritime, Space and Cyberspace.

The Atlantic Alliance's decision was not merely an update to military terminology. It recognized a transformation that was already affecting the organization, planning and conduct of operations.

The progressive digitalization of military capabilities had in fact changed the relationship between forces deployed on the ground and the systems required to command them. Digital communications, information sharing and sensor integration now make it possible to coordinate capabilities distributed across considerable distances, reducing the time needed to identify a threat, assess it and decide on a possible response.

This evolution has led to the development of multidomain operations, known as *Multi-Domain Operations* (MDO), in which land, air, naval, space and cyber capabilities are integrated to achieve coordinated effects.

The principle underlying this approach is that superiority in a single domain is not always sufficient to achieve an operational outcome. A land force can benefit from air support and satellite intelligence, while the availability and security of digital links can become decisive for coordinating the entire operation.

From this perspective, the Cyber domain plays a particular role. While land forces operate on the ground and air forces in the atmospheric domain, IT infrastructure cuts across all

operational environments, connecting their functions and capabilities.

Information superiority therefore becomes a fundamental component of military superiority. It does not simply mean possessing a greater quantity of data, but being able to collect reliable information, process it, protect it, and make it available to decision-makers when needed.

Ukraine and the tangible demonstration of warfare in cyberspace

The war between Russia and Ukraine has provided one of the most significant demonstrations of the integration between cyber operations and conventional military activities.

On February 24, 2022, about an hour before the Russian invasion began, a cyberattack struck the KA-SAT satellite communications network operated by Viasat. The operation disrupted service for thousands of users in Ukraine and tens of thousands of connections elsewhere in Europe.

On May 10 of the same year, the European Union officially attributed the attack to the Russian Federation, stating that the operation had helped facilitate the military aggression.

The incident is particularly important because it demonstrates how an action conducted in cyberspace can precede a conventional offensive and help prepare the operational conditions.

The attack did not destroy the satellite or directly compromise its onboard systems. According to the technical account published by Viasat, the attackers exploited a vulnerable configuration in a VPN device to gain access to the management network and issue commands that rendered numerous user modems unusable.

It was therefore a compromise of ground-based satellite communications management systems, with consequences extending across a far wider geographical area than that directly affected by military operations.

The KA-SAT case highlights a central aspect of contemporary warfare: a cyber operation can compromise a strategic capability without physically striking the infrastructure that makes it available.

During the conflict, both sides have had to address the need to protect their communications, keep information available, and operate in an environment characterized by cyberattacks and

intense electronic warfare.

The large-scale use of drones, reconnaissance systems, and digital platforms to coordinate units has further underscored the importance of communications and data security.

At the same time, the war in Ukraine has demonstrated the limits of cyber operations. The ability to restore systems, use alternative infrastructure, and adapt operating procedures has often made it possible to contain the effects of attacks. Cyberspace has not replaced the use of conventional force, but it has changed the conditions under which it is employed.

Command and control as a strategic target

To fully understand the importance assumed by the Cyber domain, it is necessary to consider how modern command-and-control systems—commonly identified by the acronym C2, *Command and Control*—function.

Every military operation requires a continuous flow of information between commands and subordinate units. Commanders must know the location of their own forces, receive data on the adversary, assess how the situation is developing, and transmit decisions and orders.

Digitalization has greatly increased the speed at which this information can be distributed and used, enabling coordination that previously required much more time.

However, this same evolution has introduced new vulnerabilities.

When an essential function depends on IT infrastructure, compromising that infrastructure can become an operational problem. A disrupted connection can slow the transmission of orders; an unavailable information system can reduce situational awareness; altered data can undermine the reliability of command assessments.

The effect of a cyber operation, therefore, does not necessarily have to be measured in terms of physical destruction.

Under certain circumstances, disrupting an information flow may be enough to delay a maneuver, hinder the coordination of multiple units, or temporarily limit the employment of a military capability.

This does not mean that military networks are easily penetrated. The most sensitive systems can be protected through segmentation, redundancy, encryption, and alternative procedures, including solutions that do not rely on connections to public networks.

However, increasing technological complexity makes information protection a responsibility that extends far beyond IT specialists.

The security of the command-and-control system is now an integral part of a unit's ability to carry out its mission.

A modern armed force must therefore be able not only to use available technologies effectively, but also to continue operating when some of them are compromised, disrupted, or made unavailable.

When conflict extends beyond the battlefield

One of the elements that distinguishes cyberspace from traditional military domains is its relationship with civilian infrastructure.

Modern societies depend on digital systems for energy distribution, telecommunications, transportation, industrial production, food supply, and the functioning of essential services.

Many of these infrastructures are also closely linked to the capabilities needed to sustain a military operation, either directly or through services provided by commercial operators.

As a result, the vulnerability of a civilian network can also take on strategic significance from a national defense perspective.

A recent example comes from France, where in October 2026 a cyberattack compromised the refrigeration systems of numerous supermarkets, resulting in the loss of food products and substantial economic damage.

Reports published on October 14 and 15 describe the manipulation of Internet-connected control systems used to manage the operation of refrigeration plants. Reuters reported that around 350 stores were affected, while other accounts indicated a higher number of facilities impacted by the disruptions.

Responsibility for the operation has not yet been publicly established, and there is insufficient evidence to characterize it as a military attack or attribute it to a state.

The incident is nevertheless significant because of the material consequences caused by the compromise of digital systems.

No infrastructure was bombed, and explosives were not required to disrupt economic activity. The effects resulted from altering the operation of computer-controlled industrial equipment.

This link between the digital and physical worlds represents one of the key security challenges facing modern infrastructure.

Similar systems, albeit with different characteristics and levels of protection, are used to manage energy, industrial processes, transportation, and numerous other essential activities.

Their compromise can have economic and operational consequences and, in the most serious cases, may also pose risks to public safety.

The issue is not limited to the civilian sector. The Armed Forces depend, to varying degrees, on national and commercial infrastructure for transportation, supplies, communications, and logistical support.

The ability to sustain a prolonged conflict is therefore also tied to the resilience of the country's industrial base and services.

Within this framework, the defense of cyberspace extends beyond the protection of individual military networks and becomes a component of national security.

NATO and the transformation of digital defense

The growing interdependence between military capabilities and digital infrastructure has led NATO to progressively strengthen its approach to cyber defense.

In 2024, the Allies agreed to establish the NATO Integrated Cyber Defence Centre, with the aim of improving network protection, threat awareness, and the integration of the cyber domain into the planning and conduct of operations.

On January 13, 2026, the Alliance also published the new *Alliance Digital Strategy*, a document outlining the direction of NATO's digital transformation with a long-term vision through 2035.

The strategy places particular emphasis on the ability to maintain information and decision superiority through secure, resilient, and interoperable digital infrastructure.

The planned transformation is not limited to modernizing technological systems. It encompasses the organization of information, data management, the integration of artificial intelligence, interoperability among allied forces, and the ability to keep essential functions operational even under degraded communications conditions.

The document also calls for adopting *Zero Trust* principles, based on continuous access verification and least-privilege controls, as well as the need to establish redundant systems and alternative solutions to ensure mission continuity.

The objective is to ensure that commanders can continue receiving information, making decisions, and directing forces even when part of the digital infrastructure has been compromised.

This approach highlights a major shift in the very concept of operational readiness. Alongside the availability of personnel, equipment, ammunition, and logistics capabilities, increasing importance is being placed on the ability to protect and keep operational the information systems on which military activity depends.

The change also affects personnel training. Specialized IT skills remain indispensable, but awareness of digital vulnerabilities and the ability to operate in technologically degraded conditions must also be incorporated into the training of conventional units.

A competition that may precede armed conflict

Cyberspace also introduces a different temporal dimension from conventional warfare.

Preparation for a cyber operation can begin well before the outbreak of hostilities, through network reconnaissance, vulnerability identification, information gathering, and attempts to gain access to infrastructure considered strategic.

Some of these activities may be attributable to espionage, others to cybercrime or political pressure campaigns. Not every intrusion constitutes military preparation, and attributing responsibility requires technical and intelligence assessments.

However, the possibility that a state actor may seek to gain access that can be used in a later crisis represents a significant national security concern.

Cyberspace makes it possible to conduct hostile activities even in the absence of open armed conflict, making the distinction between strategic competition, espionage, and military operations less clear-cut.

This characteristic also raises legal issues.

NATO recognizes that a particularly severe cyberattack could, under certain circumstances, lead to the invocation of Article 5 of the North Atlantic Treaty concerning collective defense.

However, there is no automatic mechanism that turns any cyberattack into an armed attack. The assessment depends on the circumstances, the effects produced, and the political decisions of allied states.

What remains true is that the ability to exert pressure against another country's infrastructure and institutions does not necessarily require moving military forces across a border.

This is one reason why cybersecurity is now considered an integral part of deterrence and defense preparedness.

The future of conflict and the role of the land domain

The growing centrality of cyberspace must not lead to an underestimation of the lessons of conventional warfare.

The conflict in Ukraine continues to demonstrate that control of territory, maneuver capability, firepower, ammunition availability, and logistical endurance remain decisive factors.

The use of new technologies has not eliminated the need to seize and defend positions, protect supply lines, and sustain units engaged in operations.

It has, however, profoundly changed the conditions under which these activities are carried out.

An army equipped with advanced assets but unable to protect its communications and maintain reliable command systems may lose some of the advantage provided by its technological superiority.

Likewise, a force equipped with less sophisticated systems but able to adapt quickly, disperse its infrastructure, and maintain operational continuity may demonstrate greater resilience than the characteristics of its available equipment alone would suggest.

The challenge, therefore, is not to shift warfare from the land domain to cyberspace, but to integrate the latter into operational preparation and conduct without creating excessively vulnerable technological dependencies.

Future military superiority will also depend on the ability to effectively combine conventional power, intelligence, digital security, and organizational resilience.

War is no longer fought only on the ground

The transformation underway requires a reassessment of how a state's military power is evaluated.

The number of tanks, aircraft, naval units, and personnel continues to provide important indications of the strength of the Armed Forces, but it does not alone describe the ability to employ these resources effectively.

The availability of secure networks, resilient communications systems, reliable intelligence, and dependable digital infrastructure is now an essential component of operational effectiveness.

A cyberattack is not necessarily capable of achieving the same results as a conventional offensive, just as compromising a network does not automatically amount to neutralizing a military force.

But cyberspace has created new opportunities to shape an adversary's operations, interfere with its capabilities, and influence the preparation and continuation of a conflict.

The land domain remains one of the environments in which the outcome of war is decided. The cyber domain, however, has become a component on which the very ability to fight effectively on land, in the air and at sea may depend.

This is the most significant transformation: the front line no longer necessarily coincides with the place where soldiers are deployed.

It can extend to communications networks, command systems, energy infrastructure and the services that support a country's military and industrial apparatus.

Twenty-first-century warfare will continue to require soldiers, equipment and conventional capabilities. But an increasingly important share of the conditions that determine their employment will also be shaped in cyberspace, often well before opposing forces come into contact.