Information-Technological Factor in Modern Conflicts: Transformation of Security and Defense Systems

Інформаційно-технологічний чинник у сучасних конфліктах: трансформація систем безпеки та оборони

Zafar Nuri Najafov
PhD., Associate Professor, e-mail zafarnajafov@yahoo.com, ORCID ID: https://orcid.org/0000-0002-1392-9559
National Defence University, Baku, Republic of Azerbaijan

Зафар Нурі Наджафов
PhD., Associate Professor, e-mail zafarnajafov@yahoo.com, ORCID ID: https://orcid.org/0000-0002-1392-9559
Національний університет оборони, Баку, Азербайджан

Received: July 30, 2026 | Revised: August 28, 2026 | Accepted: August 31, 2026

UDC 355.02:004

DOI: https://doi.org/10.33445/sds.2026.16.4.12

Purpose. This study aims to assess the role of the information-technological factor in the transformation of modern armed conflicts and determine its impact on national security and defense systems. It examines how digital technologies, cyber capabilities, artificial intelligence, unmanned systems, and strategic communications influence contemporary security environments.

Methodology. The study employs a qualitative comparative research design that combines systems, comparative, and SWOT analyses. Three conflict cases are examined: the 2020 Second Karabakh War, the Russia–Ukraine War since 2022, and selected Middle Eastern conflicts. The analysis focuses on information superiority, cyber capabilities, intelligence systems, unmanned technologies**, and cognitive influence mechanisms.**

Findings. The study indicates that information technologies have evolved from supporting military instruments into strategic components of national security systems. The comparative analysis identifies three distinct models of technological transformation: information technologies as an operational force multiplier, as the foundation of multidomain warfare, and as instruments of hybrid and asymmetric influence.

Theoretical implications. The study broadens the understanding of military transformation by integrating information security, cyber resilience, and strategic communications into the concept of contemporary security capability.

Practical implications. The findings emphasize the need to develop integrated national security systems based on digital resilience, cybersecurity capabilities, technological adaptation, and effective information management.

Value. The article provides a comparative framework for explaining how information-technological superiority affects different types of modern conflicts and contributes to the development of security studies.

Article type: Research article (qualitative comparative study).

Key words: Information Security; Military Transformation; Cyber Security; Hybrid Warfare; Artificial Intelligence; Strategic Communication; National Security.

Мета роботи. Оцінювання ролі інформаційно-технологічного чинника у трансформації сучасних збройних конфліктів та визначення його впливу на системи національної безпеки й оборони. Розглянуто, як цифрові технології, кіберспроможності, штучний інтелект, безпілотні системи та стратегічні комунікації впливають на сучасне безпекове середовище.

Метод дослідження. У дослідженні застосовано якісний порівняльний дизайн, що поєднує системний, порівняльний та SWOT-аналіз. Розглянуто три випадки збройних конфліктів: Другу карабаську війну 2020 року, російсько-українську війну з 2022 року та окремі конфлікти на Близькому Сході. Аналіз зосереджено на інформаційній перевазі, кіберспроможностях, розвідувальних системах, безпілотних технологіях і механізмах когнітивного впливу.

Результати дослідження. Дослідження свідчить, що інформаційні технології еволюціонували від допоміжних військових інструментів до стратегічних складових систем національної безпеки. Порівняльний аналіз дав змогу визначити три відмінні моделі технологічної трансформації: інформаційні технології як засіб підвищення оперативної ефективності, як основу багатодоменних воєнних дій та як інструменти гібридного й асиметричного впливу.

Теоретичне значення. Дослідження розширює розуміння військової трансформації шляхом інтеграції інформаційної безпеки, кіберстійкості та стратегічних комунікацій у концепцію сучасної безпекової спроможності.

Практичне значення. Результати підкреслюють необхідність розвитку інтегрованих систем національної безпеки, заснованих на цифровій стійкості, кібербезпекових спроможностях, технологічній адаптації та ефективному управлінні інформацією.

Оригінальність / наукова новизна. Стаття пропонує порівняльну рамку для пояснення того, як інформаційно-технологічна перевага впливає на різні типи сучасних конфліктів, і робить внесок у розвиток безпекових досліджень.

Тип статті: Дослідницька стаття (якісне порівняльне дослідження).

Ключові слова: інформаційна безпека; військова трансформація; кібербезпека; гібридна війна; штучний інтелект; стратегічні комунікації; національна безпека.

Introduction

The rapid development of information and communication technologies has fundamentally changed the nature of security threats and the mechanisms through which states ensure national

defense. Historically, military superiority was primarily associated with numerical strength, industrial capacity, territorial control, and firepower. However, contemporary conflicts demonstrate that the ability to acquire, process, protect, and use information has become a critical component of strategic power.

The digital transformation of society has created a new security environment in which physical and virtual domains are increasingly interconnected. Modern conflicts are no longer limited to traditional military confrontation; they also involve cyber operations, information influence campaigns, electronic warfare, satellite-based intelligence, artificial intelligence-supported decision-making, and cognitive operations. Consequently, information superiority has become an important component of national security and defense capabilities.

According to Alberts, Garstka, and Stein (1999), the concept of network-centric warfare demonstrates that military effectiveness increasingly depends on the ability to integrate sensors, communication systems, decision-making structures, and operational forces into a unified information network. This approach has changed the traditional understanding of command and control by emphasizing speed, connectivity, and situational awareness.

The development of cyber capabilities has further expanded the security environment. Cyber operations can affect military systems, critical infrastructure, government institutions, and social stability without direct physical confrontation. As Nye (2017) notes, cyberspace has created new forms of strategic interaction in which deterrence, vulnerability, and power projection operate differently from those in traditional military domains.

Recent conflicts provide important evidence of this transformation. The 2020 Second Karabakh War demonstrated the effectiveness of integrating unmanned aerial systems, precision weapons, intelligence capabilities, and digital command-and-control structures. The conflict showed that technological integration can significantly increase operational effectiveness and alter traditional military balances.

The Russia–Ukraine War represents a more complex stage of information-technological transformation. In this conflict, satellite-based intelligence, cyber operations, electronic warfare, open-source intelligence, artificial intelligence-based analysis, and strategic communications have become integral components of warfare. According to Watling and Reynolds (2023), the conflict illustrates the growing importance of technological adaptation and information advantage in prolonged military confrontation.

Middle Eastern conflicts demonstrate another dimension of this transformation. In these environments, information technologies are frequently used as instruments of asymmetric warfare, political influence, and psychological operations. Non-state actors and regional powers employ digital platforms, unmanned systems, and information campaigns to compensate for disparities in conventional military capabilities.

Despite extensive research on cyber warfare, artificial intelligence, and military technologies, a research gap remains concerning the comparative assessment of the information-technological factor under different conflict conditions. Existing studies often analyze individual technologies, whereas fewer examine information-technological transformation as a comprehensive security phenomenon.

Therefore, this study aims to answer three research questions:

RQ1: How has the information-technological factor transformed modern security and defense systems?

RQ2: What differences exist in the application of information technologies across conventional, large-scale interstate, and asymmetric conflicts?

RQ3: Under what conditions does information superiority become a decisive element of national security?

The main hypothesis of the study is as follows:

H1: The strategic impact of information technologies depends not only on their availability but also on the ability of states to integrate digital capabilities into resilient security and defense management systems.

Literature Review

1. Information-Technological Transformation and the Evolution of Security Concepts

The transformation of the contemporary security environment has been closely associated with the growing importance of information resources, digital infrastructure, and technological capabilities. Traditional approaches to national security primarily emphasized military power, territorial defense, and economic potential. However, the development of information and communication technologies has broadened the understanding of security by introducing new domains of competition, including cyberspace, the information space, and the cognitive environment.

The concept of security transformation suggests that technological developments do not simply provide new tools for existing military structures; rather, they change the organizational principles, decision-making processes, and strategic priorities of states. According to Buzan, Wæver, and de Wilde (1998), modern security should be understood through a broader framework that includes military, political, economic, societal, and environmental dimensions. In this context, information technologies have become a cross-sectoral factor influencing multiple security domains.

The increasing dependence of states on digital infrastructure has created new vulnerabilities. Critical infrastructure, government institutions, financial systems, and defense networks increasingly rely on information systems. Consequently, cybersecurity and information resilience have become essential elements of national security strategies (Choucri, 2012; Deibert, 2013).

The emergence of digital technologies has also changed the relationship between military and information power. Modern states increasingly compete not only through physical capabilities but also through their ability to generate information advantages, protect digital ecosystems, and influence perceptions. As Nye (2017) argues, cyber capabilities have created a new dimension of strategic competition in which power is exercised through networks, information flows, and technological dependence.

2. Information Superiority and Network-Centric Warfare

One of the most influential theoretical approaches explaining the role of information technologies in military transformation is the concept of network-centric warfare. This concept holds that military effectiveness depends on the integration of information systems, sensors, communication networks, and decision-making structures into a unified operational environment.

According to Alberts, Garstka, and Stein (1999), network-centric warfare creates operational advantages through improved situational awareness, faster decision cycles, and enhanced coordination among military units. Information superiority enables commanders to reduce uncertainty, identify opportunities, and respond more rapidly than their adversaries.

The development of network-centric approaches represents a transition from platform-centric warfare to information-based operations. In traditional military models, individual weapon systems were regarded as the main source of combat effectiveness. In contrast, contemporary military effectiveness increasingly depends on the interaction among platforms, information networks, and command structures (Cebrowski & Garstka, 1998).

However, scholars have also emphasized the limitations of technology-driven approaches. Gartzke (2013) argues that cyber and information capabilities should not be viewed as independent substitutes for traditional military power. Instead, their effectiveness depends on organizational adaptation, strategic planning, and institutional capacity.

Therefore, information superiority should be understood not merely as the possession of advanced technologies but as the ability to transform information into strategic decisions and operational outcomes.

3. Cybersecurity and Cyber Warfare as Components of National Security

The emergence of cyberspace as a domain of strategic competition has significantly influenced contemporary security studies. Unlike traditional military environments, cyberspace enables actors to conduct operations across geographical boundaries with relatively limited physical presence.

Cyber operations can target military command systems, communication networks, energy infrastructure, financial institutions, and public information systems. This has transformed cybersecurity from a primarily technical issue into a central element of national security policy (Clarke & Knake, 2012).

Kello (2017) argues that cyberspace represents a unique strategic environment in which traditional concepts of deterrence and conflict require reconsideration. The difficulty of attribution, the involvement of non-state actors, and the possibility of continuous low-level attacks complicate traditional security approaches.

The legal and strategic implications of cyber operations have also been widely discussed. Schmitt (2017) emphasizes that cyber activities create complex challenges concerning sovereignty, state responsibility, and the application of international law.

Kostyuk and Brantly (2022) highlight the role of interstate cooperation in Ukraine's cyber defense while identifying the constraints that limit its effectiveness.

4. Artificial Intelligence, Autonomous Systems, and Military Decision-Making

Artificial intelligence (AI) has become one of the most significant technological factors influencing future security environments. AI systems enable faster data processing, predictive analysis, decision support, and improved intelligence capabilities.

Horowitz (2018) argues that artificial intelligence may influence the balance of power by changing the relationship between technological innovation and military effectiveness. States capable of integrating AI into defense systems may gain significant advantages in intelligence analysis, logistics, surveillance, and operational planning.

The application of autonomous systems, especially unmanned aerial vehicles (UAVs), has already demonstrated a transformative impact on contemporary conflicts. The 2020 Second Karabakh War highlighted the operational effectiveness of integrating UAVs with intelligence and precision-strike systems.

However, the development of autonomous military technologies raises ethical, legal, and security concerns. Scharre (2018) emphasizes that autonomous weapons require careful consideration of human control, accountability, and escalation risks.

Thus, AI and autonomous systems should be considered not only as technological innovations but also as factors influencing future security doctrines and defense planning.

5. Hybrid Warfare, Information Operations, and Cognitive Security

Contemporary conflicts increasingly combine conventional military actions with information operations, cyber activities, economic pressure, and psychological influence. This phenomenon is commonly described as hybrid warfare.

Hoffman (2007) defines hybrid warfare as a combination of conventional, irregular, and cyber methods used simultaneously to achieve strategic objectives. This approach reflects the changing nature of conflict, in which military and non-military instruments are integrated.

Information operations have become a central component of hybrid warfare. Their objective is not only to disseminate information but also to influence perceptions, decision-making processes, and social behavior. According to Paul and Matthews (2016), modern disinformation campaigns exploit digital networks to create confusion, reduce trust, and influence political attitudes.

The development of social media platforms has further increased the importance of cognitive security. Singer and Brooking (2018) argue that information environments have become strategic spaces in which actors compete for influence over public perception and collective behavior.

The concept of cognitive warfare represents a further evolution of information warfare. Unlike traditional propaganda, cognitive operations aim to influence how individuals interpret information and make decisions (NATO Strategic Communications Centre of Excellence, 2023).

6. Research Gap and Theoretical Framework

The reviewed literature demonstrates that information technologies have become central elements of contemporary security and defense systems. Existing studies provide valuable insights into specific areas, such as cyber warfare, artificial intelligence, network-centric warfare, and information operations.

However, a significant research gap remains concerning the comparative evaluation of information-technological transformation across different types of armed conflicts. Many studies analyze individual technologies or specific conflicts, whereas fewer examine how the same technological factors produce different strategic effects depending on conflict characteristics.

This article addresses this gap by developing a comparative framework based on three dimensions:

1. Operational dimension – the role of information technologies in improving battlefield effectiveness.
2. Strategic dimension – the contribution of digital capabilities to national security and defense management.
3. Cognitive dimension – the influence of information technologies on perceptions, narratives, and decision-making processes.

This framework enables information-technological factors to be assessed not only as military instruments but also as broader components of contemporary security transformation.

Materials and Methods

This study employs a qualitative comparative research design to examine the role of the information-technological factor in the transformation of contemporary armed conflicts and its implications for security and defense systems.

The study is based on the assumption that information technologies have evolved from supporting military capabilities into strategic components of national security. Accordingly, it analyzes information-technological transformation not only from a military-technical perspective but also as a multidimensional security phenomenon involving defense management, cyber resilience, strategic communications, and cognitive influence.

The methodological framework combines three complementary approaches:

1. Comparative case study method.
2. Systems analysis method.
3. SWOT-based strategic assessment method.

The combination of these methods enables the identification of similarities, differences, strengths, limitations, and strategic implications of information-technological transformation across different conflict environments.

Results

The analysis indicates that information-technological capabilities have become fundamental components of contemporary security and defense systems. Whereas technological superiority was previously associated mainly with the quantity and quality of weapons platforms, modern conflicts demonstrate that strategic advantage increasingly depends on the ability to collect, process, protect, and operationalize information.

Information superiority has become a multidimensional capability integrating intelligence collection, communication networks, command-and-control systems, cyber resilience, and strategic

influence mechanisms. In this context, the critical factor is not the existence of individual technological systems but their integration into a unified security architecture.

According to Alberts et al. (1999), network-centric capabilities create advantages by improving situational awareness, accelerating decision-making processes, and enhancing coordination among operational units. Recent conflicts illustrate the relevance of this principle, as information flows influence the speed and effectiveness of military responses.

The comparative analysis identifies three distinct models of information-technological transformation:

Model 1 – Information technology as an operational force multiplier. This model characterizes conflicts in which technological capabilities significantly increase the effectiveness of conventional military operations.

Model 2 – Information technology as strategic warfare infrastructure. This model reflects conflicts in which digital capabilities influence all levels of warfare, including planning, command, logistics, intelligence, and public communication.

Model 3 – Information technology as an instrument of asymmetric and cognitive influence. This model demonstrates how technological tools enable weaker actors to compensate for conventional disadvantages through cyber operations, information campaigns, and psychological influence.

Model 3 – Information technology as an instrument of asymmetric and cognitive influence. This model demonstrates how technological tools enable weaker actors to compensate for conventional disadvantages through cyber operations, information campaigns, and psychological influence.

The 2020 Second Karabakh War provides a significant example of the operational transformation of warfare through the integration of information technologies. The conflict demonstrated how unmanned aerial systems, intelligence capabilities, precision-guided weapons, and digital command structures can fundamentally influence battlefield dynamics.

One of the defining characteristics of this conflict was the integration of reconnaissance and strike capabilities. Unmanned aerial vehicles (UAVs) provided continuous battlefield observation, target identification, and precision-engagement capabilities. This combination reduced uncertainty and increased the effectiveness of conventional military operations.

According to Najafov et al. (2023), non-kinetic capabilities were widely employed alongside kinetic means during this war. Networked sensors, unmanned aerial vehicles (UAVs), and decentralized command-and-control systems contributed to combat effectiveness. Their integration was intended to improve mission effectiveness, increase self-synchronization in the execution of actions and orders, and accelerate decision-making.

The conflict demonstrated that UAVs were not simply additional weapon systems but elements of a broader information-based operational architecture. Real-time intelligence enabled rapid decision-making and improved coordination among reconnaissance assets, artillery units, and command structures.

Cooper (2021) emphasizes that the operational significance of unmanned aerial systems in the 2020 Second Karabakh War should be assessed in conjunction with reconnaissance, artillery, and broader military planning rather than attributed to drone technology alone.

According to Bronk, Reynolds, and Watling (2022), modern conflicts increasingly demonstrate that precision-strike capabilities are most effective when combined with reliable intelligence and communication networks.

From the perspective of security transformation, the main characteristics of the information-technological factor in this conflict can be summarized as follows:

From a security transformation perspective, the main characteristics of the information-technological factor in this conflict can be summarized as follows:

The Azerbaijani case demonstrates that technological integration can yield a significant operational advantage even in a relatively limited geographic conflict environment.

The main characteristics of the information-technological factor in the Second Karabakh War are summarized in Table 1.

Table 1: Information-Technological Characteristics of the Second Karabakh War (2020)

Factor	Characteristics
Intelligence superiority	Real-time battlefield monitoring and target identification
UAV integration	Integration of surveillance and precision-strike functions
Command and control	Faster operational decision cycles
Information influence	Management of strategic narratives during and after operations

Source: *Compiled by the author based on Najafov and Gawliczek (2023) and Cooper (2021).*

However, this case also shows that technology alone does not guarantee success. The effectiveness of information systems depends on organizational adaptation, training, doctrine, and the ability to integrate different technological components into a unified operational system.

The Azerbaijani case demonstrates that technological integration can yield a significant operational advantage even in a relatively limited geographic conflict environment.

The Russia–Ukraine War represents a distinct stage in the information-technology transformation. Unlike the 2020 conflict, in which technological superiority produced rapid operational effects, the Russia–Ukraine War demonstrates the integration of digital technologies into a prolonged, multidomain confrontation.

This conflict involves:

The Russia–Ukraine War represents a distinct stage in the information-technology transformation. Unlike the 2020 conflict, where technological superiority produced rapid operational effects, the Russia–Ukraine War demonstrates the integration of digital technologies into a prolonged, multidomain confrontation.

This conflict includes:

cyber operations;

satellite-based intelligence;

electronic warfare;

open-source intelligence (OSINT);

strategic communications campaigns.

unmanned systems;

The role of commercial satellite services has become particularly important. The availability of satellite imagery and communication services has expanded intelligence capabilities beyond traditional military structures. This development demonstrates the growing role of private technology actors in contemporary security environments.

The role of commercial satellite services has become particularly important. The availability of satellite imagery and communication services has expanded intelligence capabilities beyond traditional military structures. This development demonstrates the growing role of private technological actors in contemporary security environments.

According to Kello (2017), cyberspace has transformed the relationship between technology and strategic competition by enabling states and non-state actors to influence conflicts through digital means.

The Russia–Ukraine War also demonstrates the increasing importance of cyber resilience. Cyber operations against government institutions, communication networks, and critical infrastructure have become parallel components of military confrontation.

Kostyuk and Brantly (2022) emphasize that cyber operations in contemporary conflicts are

increasingly integrated with conventional military campaigns rather than functioning as separate activities. The main characteristics of the information-technological factor in the Russia–Ukraine War are summarized in Table 2.

Table 2: Information-Technological Characteristics of the Russia–Ukraine War

Factor	Characteristics
Information superiority	Strategic-level intelligence integration
Cyber operations	Direct influence on infrastructure and governance
AI application	Data analysis and decision-support functions
OSINT	Expansion of intelligence capabilities
Strategic communications	Global information competition

Source: *Compiled by the author based on Watling and Reynolds (2023), Kostyuk and Brantly (2022), and Horowitz (2018).*

The Russia–Ukraine War demonstrates that information technologies have evolved from force multipliers into structural components of warfare.

Information Technologies in Middle Eastern Conflicts

Middle Eastern conflicts demonstrate another model of technological transformation. Unlike large-scale interstate conflicts, many conflicts in this region involve asymmetric confrontation between states and non-state actors.

In such environments, information technologies are often used to compensate for disparities in conventional military capabilities. Low-cost unmanned systems, social media platforms, cyber tools, and information campaigns enable actors with limited resources to influence political and security environments.

Bassiri Tabrizi and Bronk (2018) examine the proliferation of armed drones in the Middle East and demonstrate how these systems have expanded the military capabilities available to regional actors. Their findings provide a basis for assessing the role of unmanned technologies in asymmetric conflict environments.

Hoffman (2007) identifies hybrid warfare as a combination of conventional military methods, irregular tactics, cyber operations, and information influence mechanisms. This framework is particularly relevant to understanding contemporary Middle Eastern conflicts.

Information operations have become especially important because the management of narratives and public perceptions can influence political legitimacy and international support.

According to Paul and Matthews (2016), modern information campaigns exploit digital communication environments to create uncertainty, amplify social divisions, and influence decision-making processes. The main characteristics of the information-technological factor in the selected Middle Eastern conflicts are summarized in Table 3.

Table 3: Information-Technological Characteristics of Selected Middle Eastern Conflicts

Factor	Characteristics
Technological approach	Low-cost and adaptive technologies
Main objective	Political influence and asymmetric advantage
Information operations	Narrative management and psychological impact
Cyber dimension	Supporting and selective application

Source: *Compiled by the author based on Bassiri Tabrizi and Bronk (2018), Hoffman (2007), and Paul and Matthews (2016).*

Therefore, Middle Eastern conflicts demonstrate that information technologies are not only instruments of technologically advanced states but also tools available to weaker actors seeking strategic influence.

Comparative Assessment of Information-Technological Factors

The comparative analysis reveals significant differences in the role of information technologies across the three conflict environments.

The comparative characteristics of the three conflict environments are presented in Table 4.

Table 4: Comparative Assessment of Information-Technological Factors Across Three Conflict Environments

Dimension	Second Karabakh War (2020)	Russia–Ukraine War	Middle Eastern Conflicts
Main role of technology	Operational advantage	Strategic warfare infrastructure	Asymmetric influence
Information superiority	Battlefield-focused	Strategic and operational	Political and cognitive
UAV application	Precision strike and reconnaissance	Mass deployment and adaptation	Resource-efficient asymmetric tool
Cyber dimension	Limited supporting role	Major strategic domain	Selective application
Information operations	Supporting element	Integrated warfare component	Core influence mechanism

Source: *Compiled by the author based on Najafov and Gawliczek (2023), Cooper (2021), Watling and Reynolds (2023), Kostyuk and Brantly (2022), Bassiri Tabrizi and Bronk (2018), Hoffman (2007), and Paul and Matthews (2016).*

The analysis identifies a progressive development pattern in information-technological transformation:

First stage: Information technologies increase battlefield effectiveness.

Second stage: Information technologies become integrated into national defense and security systems.

Third stage: Information technologies become instruments of political influence, cognitive competition, and hybrid warfare.

Discussion of Findings

The results support the hypothesis that the strategic impact of information technologies depends not only on their availability but also on institutional capacity, organizational adaptation, and security governance.

The comparison demonstrates that the same technologies may produce different outcomes depending on the conflict environment.

For example:

UAV systems produced decisive operational effects in the 2020 Second Karabakh War because they were integrated with intelligence and precision-strike systems.

In the Russia–Ukraine War, UAVs became widely deployed systems within a broader technological ecosystem involving electronic warfare, cyber operations, and intelligence networks.

In Middle Eastern conflicts, similar technologies often serve as asymmetric instruments for actors seeking political and psychological influence.

Therefore, information-technological superiority should be understood as a systemic capability rather than a collection of separate technologies.

Discussion

The findings of this study indicate that the information-technological factor has become a structural element of contemporary security systems rather than merely a supporting capability of military organizations. The comparative analysis of the Second Karabakh War (2020), the Russia–Ukraine War (2022–present), and Middle Eastern conflicts indicates that information technologies influence

modern conflicts through different mechanisms depending on the political, military, and technological context.

A key theoretical implication of this study is that information superiority should be considered an independent dimension of strategic power. Traditional approaches to military capability emphasized physical resources, including manpower, weapons systems, industrial capacity, and territorial control. However, contemporary conflicts indicate that the ability to generate, process, protect, and exploit information increasingly determines the effectiveness of these traditional capabilities.

This finding is consistent with the concept of network-centric warfare developed by Alberts, Garstka, and Stein (1999), according to which information connectivity creates operational advantages by reducing uncertainty and accelerating decision cycles. Nevertheless, the results of this study suggest that the concept requires further expansion. In contemporary security environments, information superiority is no longer limited to battlefield effectiveness; it includes cyber resilience, strategic communications, public perception management, and protection against cognitive manipulation.

The comparative analysis also demonstrates that technological superiority alone cannot determine conflict outcomes. The effectiveness of information technologies depends on institutional capacity, organizational flexibility, doctrinal adaptation, and human expertise. This conclusion supports the argument of Gartzke (2013), who emphasized that cyber and technological capabilities should not be viewed as independent substitutes for traditional power but as components of broader strategic systems.

The Second Karabakh War (2020) represents a case in which information technologies acted primarily as an operational force multiplier. The integration of UAVs, intelligence systems, and precision weapons demonstrated how technological synchronization can transform battlefield dynamics. However, the experience also indicates that the decisive factor was not the possession of individual systems but their integration into an effective command-and-control structure.

The Russia–Ukraine War represents a more advanced stage of transformation. In this conflict, information technologies influence all levels of warfare, from tactical operations to strategic communications and international diplomacy. The extensive use of satellite-based intelligence, cyber operations, OSINT, electronic warfare, and digital communications demonstrates that modern conflicts increasingly occur within a multidomain environment in which physical and virtual spaces are interconnected.

This observation is consistent with contemporary security studies emphasizing that cyberspace has become an independent strategic domain. As Nye (2017) argues, cyber capabilities have changed traditional concepts of deterrence and strategic competition by creating new forms of influence and vulnerability.

The analysis of Middle Eastern conflicts reveals another important dimension: information technologies enable asymmetric actors to achieve strategic effects despite conventional disadvantages. Hybrid warfare approaches combine military, informational, cyber, and political instruments to influence both adversaries and wider audiences (Hoffman, 2007). In such environments, managing narratives and shaping perceptions may become as important as achieving territorial gains.

Another important finding concerns the relationship between information warfare and cognitive security. Modern information operations increasingly target not only information systems but also human decision-making processes. The development of social media platforms, algorithmic communication environments, and artificial intelligence-based content generation has expanded the possibilities for manipulation and influence.

According to Singer and Brooking (2018), digital communication platforms have transformed information environments into strategic spaces in which political and security competition takes

place. Therefore, contemporary national security strategies must include not only cyber defense but also cognitive resilience and strategic communications capabilities.

The study contributes to the existing literature in three ways.

First, it develops a comparative framework that evaluates information-technological transformation across different conflict models rather than analyzing individual technologies separately.

Second, it demonstrates that information technologies perform different strategic functions depending on conflict conditions:

operational advantage in limited high-intensity conflicts;

structural integration in large-scale interstate warfare;

asymmetric influence in hybrid conflicts.

Third, it broadens the understanding of national security by integrating military transformation, cybersecurity, and cognitive security into a unified analytical framework.

Conclusion

This study examined the role of the information-technological factor in the transformation of modern armed conflicts and evaluated its implications for security and defense systems through a comparative analysis of three conflict cases.

The findings indicate that information technologies have become decisive components of contemporary strategic capability. Their importance is determined not only by technological innovation itself but also by the ability of states and organizations to integrate digital systems into effective security architectures.

The main conclusions of the study are as follows.

First, information superiority has become an independent component of national security capability. It includes intelligence collection, information processing, communication systems, cyber resilience, and strategic influence mechanisms.

Second, modern military effectiveness increasingly depends on the integration of technological systems rather than the possession of individual weapons platforms. UAVs, artificial intelligence, satellite systems, and cyber capabilities produce strategic effects when combined within a coherent operational and organizational framework.

Third, the comparative analysis identifies different models of information-technological transformation:

1. Operational transformation model – represented by the 2020 Second Karabakh War, in which information technologies increased battlefield effectiveness through intelligence integration and precision operations.

2. Strategic transformation model – represented by the Russia–Ukraine War, in which digital capabilities have become fundamental components of military planning, command, intelligence, and international information competition.

3. Hybrid transformation model – represented by Middle Eastern conflicts, in which information technologies serve as instruments of asymmetric warfare, political influence, and cognitive operations.

Fourth, cyberspace has become an essential dimension of national security. The increasing dependence of states on digital infrastructure requires the development of cyber resilience, protection mechanisms, and integrated security strategies.

Fifth, the role of information-psychological and cognitive operations demonstrates that future conflicts will increasingly involve competition over perceptions, narratives, and decision-making processes. Therefore, information security must include not only technical protection but also societal resilience against manipulation.

Sixth, artificial intelligence, autonomous systems, and big data analytics will continue to transform security environments. However, technological development must be accompanied by ethical standards, legal regulation, and effective human control mechanisms.

The study concludes that the future character of warfare will be determined not solely by technological superiority but also by the ability to create integrated, resilient, and adaptive security systems capable of combining military, cyber, informational, and cognitive capabilities.

Thus, information-technological transformation should be considered one of the central factors shaping the evolution of national security concepts in the twenty-first century.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

Use of Artificial Intelligence

Artificial intelligence tools were used solely for technical text checking.

References

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network centric warfare: Developing and leveraging information superiority*. CCRP Publication Series.

Allied Command Transformation. (2023, April 5). *Cognitive warfare: Strengthening and defending the mind*. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

Bassiri Tabrizi, A., & Bronk, J. (2018). *Armed drones in the Middle East: Proliferation and norms in the region*. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/occasional-papers/armed-drones-middle-east-proliferation-and-norms-region

Bronk, J., Reynolds, N., & Watling, J. (2022). *The Russian air war and Ukrainian requirements for air defence*. Royal United Services Institute.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cebrowski, A. K., & Garstka, J. J. (1998). Network-centric warfare: Its origin and future. *Proceedings, 124*(1), 28–35. https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future

Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press.

Clarke, R. A., & Knake, R. K. (2012). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

Cooper, J. (2021). *The Nagorno-Karabakh war: A spur to Moscow's UAV efforts?* International Institute for Strategic Studies. https://www.iiss.org/research-paper/2021/03/nagorno-karabakh-war-moscow-uav-efforts/

Deibert, R. (2013). *Black code: Inside the battle for cyberspace*. McClelland & Stewart.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security, 38*(2), 41–73. https://doi.org/10.1162/ISEC_a_00124

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review, 1*(3), 36–57. https://doi.org/10.15781/T2639KP49

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kostyuk, N., & Brantly, A. (2022). War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation. *Contemporary Security Policy, 43*(3), 498–515. https://doi.org/10.1080/13523260.2022.2093587

Najafov, Z., & Gawliczek, P. J. (2023). The signs of the Second Karabakh War typical of the 5th generation war. *Civitas et Lex, 38*(2), 19–30. https://doi.org/10.31648/cetl.8652

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Paul, C., & Matthews, M. (2016). *The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it*. RAND Corporation. https://doi.org/10.7249/PE198

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company. https://wwnorton.com/books/Army-of-None/

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt. https://www.hachettebookgroup.com/titles/p-w-singer/likewar/9781328695741/

Watling, J., & Reynolds, N. (2023). *Meatgrinder: Russian tactics in the second year of its invasion of Ukraine*. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine